ViPNet Business Mail 4.3

Benutzerhandbuch



Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Version: 00116-04 34 03 DEU

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt



Einführung

Über dieses Dokument

Zielgruppe

Das vorliegende Handbuch ist für Benutzer der Anwendung ViPNet Business Mail sowie für Administratoren des ViPNet–Netzwerks bestimmt. Das Handbuch enthält eine Benutzeranleitung und Hinweise zur Konfiguration des Programms.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Über das Programm

Das Programm ViPNet Business Mail wird dazu verwendet, elektronische Nachrichten im geschützten ViPNet Netzwerk (s. ViPNet Netzwerk auf S. 180) auszutauschen. Diese Funktionalität kann nur von denjenigen Benutzern des ViPNet Netzwerks verwendet werden, die eine Verbindung miteinander haben.

Das Programm „Business Mail" ist ein Teil der ViPNet Client Software und kann sowohl gemeinsam mit anderen Komponenten des Programmpakets als auch einzeln auf dem Rechner installiert werden. Die Installation der ViPNet Client Software ist im Handbuch „ViPNet Client Monitor. Benutzerhandbuch" beschrieben.

„Business Mail" beinhaltet die Standardfunktionalitäten eines Mail–Clients:

- Senden und Empfangen von Nachrichten.
- Senden und Empfangen von Nachrichten mit Anhängen.
- Signieren von Nachrichten und Anhängen mit digitaler Signatur.
- Verschlüsseln von Dateien und Anhängen.

„Business Mail" hat auch einige Besonderheiten:

- Den Zugriff auf das Programm an einem ViPNet–Netzwerkknoten hat nur der Benutzer dieses Knotens.
- Die Nachrichten von „Business Mail" werden im ViPNet–Netzwerk mit Hilfe des MFTP-Moduls (s. MFTP–Modul einstellen auf S. 111) über geschützte Kanäle übertragen
- Die Nachrichten von „Business Mail" sind mit dem Schlüsselsatz des Empfängers (s. Ebenen der Adressierung auf S. 37) und können daher von niemand anderem gelesen werden
- „Business Mail" hat ein ausgefeiltes System zur automatischen Verarbeitung von eingehenden Mails und ausgehenden Dateien (s. Autoprocessing auf S. 79).

Systemanforderungen

Die Mindestanforderungen an den Rechner für die Installation von ViPNet Business Mail sind:

- Prozessor: ein Intel Core 2 Duo oder ein anderer x86-kompatible Prozessoren mit mindestens zwei Kernen wird empfohlen.
- Mindestens 512 MB RAM.
- Mindestens 100 MB freier Speicherplatz, empfohlen sind 200 MB.
- Netzwerkadapter oder Modem.
- Betriebssysteme Windows XP (32-Bit), Server 2003 (32-Bit), Vista (32/64-Bit), Server 2008 (32/64-Bit), Server 2008 R2 (64-Bit), Small Business Server 2008 SP2 (64-Bit), Windows 7 (32/64-Bit), Windows 8 (32/64-Bit), Windows 8.1 (32/64-Bit), Server 2012 (64-Bit), Server 2012 R2 (64-Bit).

  Im Betriebssystem sollte das neueste Updatepaket installiert sein.
- Bei Verwendung früherer Windows-Versionen als Windows 8 sollte auf dem Computer das kumulative Zeitzonenupdate KB2570791 installiert werden.
- Internet Explorer ab Version 6.0.

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).



Schnellstart

Bevor Sie beginnen

Das vorliegende Kapitel beinhaltet kurze Hinweise zur Nutzung der wichtigsten Möglichkeiten von „Business Mail". Diese Informationen werden es ermöglichen, ohne ausführliches Studium dieses Benutzerhandbuchs mit der Arbeit beginnen zu können.

Um die Arbeit mit E–Mails zu beginnen, starten Sie das Programm (s. Programm starten und beenden auf S. 23). Die wichtigsten Schritte der Handhabung von E–Mails kann man weiter unten in diesem Kapitel kennenlernen. Sollten irgendwelche Schwierigkeiten auftreten, so lesen Sie den Abschnitt Arbeiten mit Nachrichten (auf S. 39).

Die Nutzung von kryptografischen Möglichkeiten des Programms wird im Kapitel Digitale Signatur und Verschlüsselung (auf S. 65) beschrieben, die automatische Verarbeitung von Nachrichten und Dateien im Kapitel Autoprocessing (auf S. 79).

Nachrichten verfassen

Führen Sie folgende Schritte aus, um eine Nachricht zu verfassen:

1. Klicken Sie im ViPNet Business Mail Hauptfenster in der Symbolleiste auf die Schaltfläche **Post**.
2. Geben Sie im Fenster **Postausgang** den Betreff und den Nachrichtentext ein. Ändern Sie bei Bedarf das Format des Nachrichtentextes.
3. Wenn an die Nachricht Dateien angehängt werden sollen, klicken Sie in der Symbolleiste auf **Anhänge** und wählen Sie im Fenster **Öffnen** die benötigten Dateien.



Hinweis. Die Gesamtgröße der hinzugefügten Anhänge darf nicht 2 GB überschreiten.

4. Wenn ein Verschlüsseln der Nachricht erforderlich ist, klicken Sie auf die Schaltfläche **Verschlüsseln**.
5. Wenn die Nachricht digital signiert werden soll, klicken Sie auf die Schaltfläche **Signieren** .
6. Klicken Sie auf die Schaltfläche **Empfänger** und wählen Sie im Fenster **Adressbuch** die Empfänger aus.
7. Klicken Sie auf die Schaltfläche **Senden**.

Weitere Informationen finden Sie unter Neue Nachricht erstellen und versenden (auf S. 40).

Nachrichten digital signieren

Führen Sie folgende Schritte aus, um die Nachricht mit einer digitalen Unterschrift zu signieren:

- Wenn die Nachricht im Fenster **Verfassen** geöffnet ist, klicken Sie in der Symbolleiste auf die Schaltfläche **Signieren** .
- Wenn die Nachricht im Ordner **Postausgang** oder einem Unterordner davon abgelegt und noch nicht versendet ist:
  - Wählen Sie die Nachricht aus der Liste.
  - Klicken Sie auf die Schaltfläche **Signieren** in der Symbolleiste des ViPNet Business Mail Hauptfensters.

Weitere Informationen finden Sie unter Nachricht digital signieren (auf S. 67).

Nachrichten lesen

Beim Empfang neuer Nachrichten gibt das MFTP–Modul eine entsprechende Meldung aus. Ungelesene Nachrichten in der Liste sind in fetter Schrift dargestellt. Ordner, die ungelesene Nachrichten enthalten, werden in „Business Mail“ ebenfalls in fetter Schrift hervorgehoben, dabei wird neben dem Namen des Ordners die Anzahl der ungelesenen Nachrichten in Klammern angezeigt.

Um eine Nachricht zu lesen:

1. Wählen Sie im ViPNet Business Mail Hauptfenster im Navigationsbereich in der Navigationsleiste den Ordner, in dem sich die Nachricht befindet.
2. Wählen Sie die Nachricht aus der Liste. Wenn die E–Mail nicht verschlüsselt ist, wird ihr Text im Bereich unterhalb der Nachrichtenliste eingeblendet.

   Wenn die Nachricht verschlüsselt ist, führen Sie für die Anzeige des Textes einen der folgenden Schritte aus:

   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Entschlüsseln** .
   - Öffnen Sie die Nachricht mit einem Doppelklick in einem separaten Fenster.

Weitere Informationen finden Sie unter Nachrichten und Anhänge im separaten Fenster anzeigen (auf S. 50).

Nachrichten beantworten

Führen Sie folgende Schritte aus, um eine E–Mail zu beantworten:

1 Wählen Sie eine Nachricht in der Liste aus oder öffnen Sie diese mit einem Doppelklick in einem separaten Fenster.

2 Klicken Sie im ViPNet Business Mail Hauptfenster oder im offenen Nachrichtenfenster in der Symbolleiste auf die Schaltfläche **Antworten** oder **Allen antworten** .

   Es wird das Fenster zum Erstellen einer Nachricht geöffnet.

3 Verfassen und versenden Sie die Nachricht wie im Abschnitt Nachrichten verfassen (auf S. 15).

Weitere Informationen finden Sie unter Nachricht beantworten und weiterleiten (auf S. 52).

Nachrichten nach Microsoft Outlook übertragen

Führen Sie einen der folgenden Schritte aus, um die Nachricht nach Microsoft Outlook oder Outlook Express (Windows Mail) zu übertragen:

- Ziehen Sie die Nachricht aus dem ViPNet Client Hauptfenster in das offene Fenster zum Erstellen einer neuen Nachricht in Microsoft Outlook oder Outlook Express. Die übertragene E–Mail wird in der neuen Nachricht als Anhang eingefügt.
- Ziehen Sie die Nachricht aus dem ViPNet Client Hauptfenster in irgendeinen Ordner im Hauptfenster von Microsoft Outlook oder Outlook Express. Im ausgewählten Ordner erscheint eine Nachricht, in die die übertragene „Business Mail" Nachricht eingefügt ist.

Weitere Informationen finden Sie unter Nachrichten exportieren und importieren (auf S. 56).

Nachrichten löschen

Führen Sie folgende Schritte aus, um eine Nachricht zu löschen:

1 Wählen Sie im ViPNet Business Mail Hauptfenster im Navigationsbereich in der Navigationsleiste den Ordner mit der Nachricht, die entfernt werden soll.

2 Wählen Sie die Nachricht aus der Liste und klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen** oder drücken Sie die **ENTF**–Taste.

   Die Nachricht wird in den Ordner **Gelöschte Objekte** verschoben, in einen Unterordner mit dem Namen des Quellordners, aus dem die Nachricht stammt.

Weitere Informationen finden Sie unter Nachrichten löschen (auf S. 59).

2

Arbeit mit dem Programm ViPNet Business Mail beginnen

Installation des Programms

Das Programm ViPNet Business Mail stellt eine Komponente der Software ViPNet Client dar. Im Rahmen des ViPNet Netzwerks auf Basis der Software ViPNet Administrator wird das Programm ViPNet Business Mail standardmäßig zusammen mit der Hauptkomponente ViPNet Monitor auf den Computer installiert. Wenn nötig, können Sie jedoch das Programm ViPNet Business Mail gesondert (ohne ViPNet Monitor) installieren. Im Rahmen der Softwarelösung ViPNet VPN wird das Programm ViPNet Business Mail getrennt vom Programm ViPNet Monitor installiert. Ausführliche Informationen zur Installation von ViPNet Client s. Dokument „ViPNet Client Monitor. Benutzerhandbuch“, Abschnitt „Installation, Update und Deinstallation von ViPNet Client“.

Außerdem sollten ViPNet Adresslisten und -Schlüssel auf dem Computer installiert sein, um das Programm ViPNet Business Mail verwenden zu können. Wenn Sie die Adresslisten und Schlüssel im Programm ViPNet Monitor installiert haben, werden diese automatisch auch im Programm ViPNet Business Mail verwendet. Wenn ViPNet Monitor nicht auf dem Computer installiert ist, dann installieren Sie vor Beginn Ihrer Arbeit mit ViPNet Business Mail die erforderlichen Adresslisten und Schlüssel mit Hilfe einer Schlüsseldistribution (Datei `*.dst`). Diese Datei erhalten Sie vom Administrator Ihres ViPNet Netzwerks. Weitere Details s. Dokument „ViPNet Client Monitor. Benutzerhandbuch“, Abschnitt „Installation und Update der Adresslisten und Schlüssel“.



Hinweis. Das Programm Business Mail kann nur auf Netzwerkknoten mit der Rolle „Business Mail“ verwendet werden. Wenn diese Rolle einem Knoten nicht zugewiesen ist, wird das Starten des Programms auf dem gegebenen Knoten nicht möglich sein.

Programm starten und beenden

Führen Sie folgende Schritte aus, um das Programm ViPNet Business Mail zu starten:

1 Für den Start von ViPNet Business Mail nutzen Sie eine der folgenden Optionen:

- Wenn die Anwendung ViPNet Monitor läuft, wählen Sie im Menü **Anwendungen** den Eintrag **Business Mail**. Es öffnet sich unmittelbar das Hauptfenster von ViPNet Business Mail. Eine Benutzerauthentifizierung ist in diesem Fall nicht nötig.
- Wenn das MFTP–Modul neue Postpakete empfängt, wird eine Meldung über den Erhalt neuer Nachrichten eingeblendet.

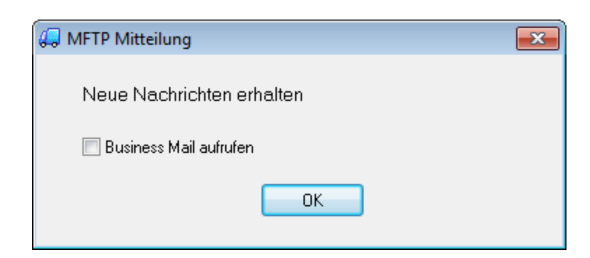


Abbildung 1. Meldung über den Erhalt neuer Nachrichten



Hinweis. Die Meldung wird nur dann eingeblendet, wenn entsprechende Einstellungen im MFTP–Modul vorgenommen wurden (siehe „ViPNet MFTP. Administratorhandbuch“).

Um das Programm ViPNet Business Mail zu starten, stellen Sie sicher, dass in der angezeigten Meldung das Kontrollkästchen **Business Mail aufrufen** aktiviert ist, und klicken Sie dann auf **OK**. Es wird das Anmeldefenster von „Business Mail“ eingeblendet.

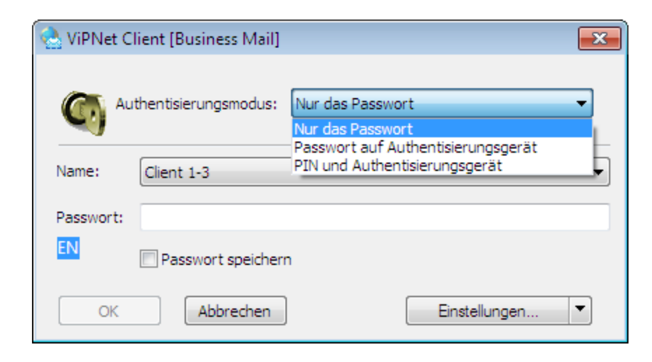


Abbildung 2. Das Anmeldefenster von ViPNet Business Mail

- Führen Sie einen der folgenden Schritte aus, um ViPNet Business Mai“ über eine Verknüpfung zu starten:
  - Verwenden Sie das Betriebssystem Windows 7, Windows Server 2008 R2 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Client** > **Business Mail**.

- Verwenden Sie das Betriebssystem Windows 8 oder Windows Server 2012, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **Business Mail**.



Hinweis. Im Zuge der Installation könnte sich die Position des Programmeintrags im Menü Start auch geändert haben.

- Doppelklicken Sie auf dem Desktop auf die Verknüpfung (die Verknüpfung wird auf dem Desktop angezeigt, wenn im Zuge der Programminstallation eine entsprechende Option gewählt wurde).

Das Anmeldefenster des Programms wird geöffnet.

2 Führen Sie im Anmeldefenster folgende Schritte aus:

2.1 In Abhängigkeit vom aktuellen Anmeldemodus (s. Authentisierungsmodi auf S. 26) geben Sie entweder das Benutzerpasswort ein oder schließen Sie ein Authentisierungsgerät an und geben Sie die PIN ein.

2.2 Nach der Eingabe aller für die Authentifizierung erforderlichen Daten klicken Sie auf **OK**. Das Hauptfenster des Programms ViPNet Business Mail wird geöffnet.

Klicken Sie auf die Schaltfläche **Minimieren** in der oberen rechten Ecke des Fensters, um das Programmfenster in der Taskleiste einzublenden.

Führen Sie einen der folgenden Schritte aus, um das Programm zu beenden:

- Klicken Sie im Hauptfenster von ViPNet Business Mail im Menü **Datei** auf **Beenden**.
- Klicken Sie auf die Schaltfläche **Schließen** in der oberen rechten Ecke des Fensters.



Hinweis. Wenn im Fenster Extras, Einstellungen im Bereich **Allgemein** (s. Allgemeine Parameter einstellen auf S. 103) das Kontrollkästchen **Zur Taskleiste minimieren** aktiviert ist, wird beim Klicken auf die Schaltfläche **Schließen** das Programmfenster in den Infobereich der Taskleiste minimiert.

Benutzer wechseln

Wenn am ViPNet–Netzwerkknoten mehrere Benutzer registriert sind, kann der Benutzer gewechselt werden, ohne das Programm ViPNet Business Mail zu verlassen. Dazu führen Sie folgende Schritte aus:

1 Klicken Sie im Hauptfenster des Programms ViPNet Business Mail im Menü **Extras** auf **Benutzer wechseln**. Es wird das Anmeldefenster eingeblendet (s. Abbildung auf S. 23).

2 Geben Sie das Passwort des neuen Benutzers ein und klicken auf **OK**.



Hinweis. Für den anzumeldenden Benutzer muss am ViPNet–Netzwerkknoten eine Schlüsseldistribution eingerichtet sein.

Authentisierungsmodi

Im Programm ViPNet Business Mail sind drei Authentisierungsmodi vorgesehen:

- Nur das Passwort (auf S. 27). Zur Anmeldung im Programm sollten Sie Ihr Benutzerpasswort eingeben. Nach jeder Eingabe des Passworts wird ein Kennwortschlüssel berechnet, der für den Zugang zu Ihrem privaten Schlüssel verwendet wird.
- Passwort auf Authentisierungsgerät (auf S. 28). Zur Anmeldung im Programm sollten Sie ein Authentisierungsgerät anschließen und eine PIN eingeben.

  In der Regel setzt die Benutzung dieses Authentisierungsmodus voraus, dass Ihr Benutzerpasswort auf dem Gerät gespeichert und Ihnen nicht bekannt ist. Wenn Sie das Passwort kennen, dann können Sie neben der Authentifizierung per Authentisierungsgerät auch das Benutzerpasswort für die Anmeldung im Programm verwenden. Diese Möglichkeit gewährleistet die Anmeldung im Programm auch dann, wenn das entsprechende Authentisierungsgerät beschädigt ist (in diesem Fall können Sie Ihr Passwort von Ihrem ViPNet Netzwerkadministrator erfahren).



Achtung! Der Authentisierungsmodus **Passwort auf Authentisierungsgerät** entspricht nicht mehr den Sicherheitsanforderungen und wird ausschließlich aus Gründen der Kompatibilität mit früheren Versionen der ViPNet-Software unterstützt. Wenn also das Programm ViPNet Business Mail auf die Version 4.x aktualisiert wurde und wenn dort der gegebene Authentisierungsmodus verwendet wird, dann empfehlen wir nachdrücklich, den Authentisierungsmodus auf **Nur das Passwort** oder **PIN und Authentisierungsgerät** zu ändern.

- PIN und Authentisierungsgerät (auf S. 29). Zur Anmeldung im Programm sollten Sie ein Authentisierungsgerät anschließen und eine PIN (in manchen Fällen auch ein Passwort) eingeben.

Standardmäßig ist der Authentisierungsmodus **Nur das Passwort** eingestellt. Im Administratormodus können Sie den Authentisierungsmodus wechseln.

In einem der Modi **Passwort auf Authentisierungsgerät** oder **PIN und Authentisierungsgerät** erfolgt die Authentifizierung anhand eines externen Speichergeräts (s. Liste externer Datenträger auf S. 175). Damit ein Gerät für die Authentifizierung des Benutzers verwendet werden kann, sollten zunächst die Treiber dieses Geräts auf dem Computer installiert und anschließend die entsprechenden Schlüssel auf dem Gerät gespeichert werden. Die Speicherung der Schlüssel auf einem externen Gerät kann bei einer Änderung des Authentisierungsmodus oder im Programm ViPNet Key and Certification Authority beim Erzeugen der Schlüsseldistribution veranlasst werden (in ViPNet Network Manager ist die Arbeit mit externen Geräten nicht möglich).



Achtung! Wenn bei Verwendung des Authentisierungsmodus **Passwort auf Authentisierungsgerät** oder **PIN und Authentisierungsgerät** das externe Gerät vom Computer getrennt wird, dann wird automatisch der Computer gesperrt – in Übereinstimmung mit den Einstellungen, die im Administratormodus vorgenommen wurden. Zum Fortsetzen der Arbeit sollte das externe Gerät wieder an den Computer angeschlossen werden.

In der Abbildung unten sind die Authentisierungsfaktoren für jeden Authentisierungsmodus dargestellt, die den unterschiedlichen Arten der Anwendung von externen Speichergeräten entsprechen.

Authentisierungsmodi

Nur das Passwort
einstufig
(nur Passwort)

Passwort auf Authentisierungsgerät
Unterstützt das Gerät eine PIN?
ja
zweistufig
(PIN +
Authentisierungsgerät)
nein
einstufig
(nur
Authentisierungsgerät)

PIN und Authentisierungsgerät
Unterstützt das Gerät
den Standard PKCS#11?
ja
Zertifikat und privater Schlüssel
auf Gerät gespeichert?
ja
zweistufig
(PIN + Zertifikat
auf Authentisierungsgerät)
nein
zweistufig
(PIN +
Authentisierungsgerät)
nein
Unterstützt das Gerät
eine PIN?
ja
Kennwortschlüssel
auf Gerät gespeichert?
ja
zweistufig
(PIN +
Authentisierungsgerät)
nein
zweistufig
(Passwort und PIN
+ Authentisierungsgerät)
nein
Kennwortschlüssel
auf Gerät gespeichert?
ja
einstufig
(nur
Authentisierungsgerät)
nein
zweistufig
(Passwort +
Authentisierungsgerät)

Bei Verwendung dieses Authentisierungsmodus wird der private Schlüssel des Benutzers durch die PIN des externen Datenträgers geschützt. In allen anderen Fällen wird der private Benutzerschlüssel durch den Kennwortschlüssel geschützt.

Abbildung 3. Übersicht der Zusammenhänge zwischen Authentisierungsmodi und Authentisierungsstufen

Nur das Passwort

Führen Sie im Anmeldefenster von ViPNet Business Mail die folgenden Schritte aus, um sich mit Ihrem Benutzerpasswort im Programm anzumelden:

1 Wählen Sie in Liste **Authentisierungsmodus** den Eintrag **Nur das Passwort**.

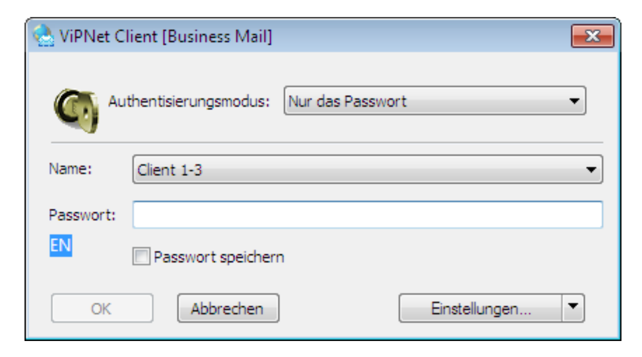


Abbildung 4. Authentisierungsmodus „Nur das Passwort"

2 Wenn nötig, wählen Sie den Namen Ihres ViPNet-Benutzers in der Liste **Name** aus.



Hinweis. In dieser Liste werden die Namen aller Benutzer aufgeführt, deren Schlüssel auf dem gegebenen Netzwerkknoten installiert wurden.Wenn keine Benutzerschlüssel auf dem Netzwerkknoten installiert ist, dann wird eine leere Liste angezeigt.

---

3 Geben Sie Ihr Passwort im Feld **Passwort** ein.

Wenn das Speichern von Passwörtern in der Registry von den Einstellungen des Programms erlaubt ist (s. Zusätzliche Sicherheitseinstellungen auf S. 115), dann kann das entsprechende Kontrollkästchen aktiviert werden.

4 Klicken Sie auf **OK**.

Passwort auf Authentisierungsgerät



Achtung! Zur Vermeidung von Störungen in der Arbeit der ViPNet Software sollte der Authentisierungsmodus **Passwort auf Authentisierungsgerät** nicht verwendet werden. Bei Verwendung dieses Authentisierungsmodus empfehlen wir, den Modus auf **Nur das Passwort** oder **PIN und Authentisierungsgerät** zu ändern.

Führen Sie im Anmeldefenster von ViPNet Business Mail die folgenden Schritte aus, um sich mit einem Passwort auf Authentisierungsgerät im Programm anzumelden

1 Wählen Sie in Liste **Authentisierungsmodus** den Eintrag **Passwort auf Authentisierungsgerät**.

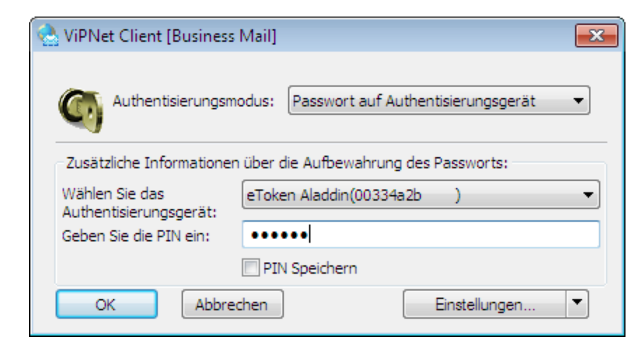


Abbildung 5. Authentisierungsmodus „Passwort auf Authentisierungsgerät“

2 Schließen Sie das externe Gerät, auf dem sich Ihr Passwort befindet, an den Computer an.

3 Wählen Sie das benötigte externe Gerät in der Liste **Authentisierungsgerät** aus.

4 Wenn nötig, geben Sie eine PIN ein. Ob die Eingabe einer PIN erforderlich ist, hängt vom Typ des verwendeten externen Geräts ab (s. Abbildung auf S. 27).

Damit die eingegebene PIN gemerkt wird und bei nachfolgenden Anmeldungen nicht mehr angegeben werden muss, aktivieren Sie das entsprechende Kontrollkästchen.

5 Klicken Sie auf **OK**.

PIN und Authentisierungsgerät

Führen Sie im Anmeldefenster von ViPNet Business Mail die folgenden Schritte aus, um sich mit PIN und Authentisierungsgerät im Programm anzumelden

1 Wählen Sie in Liste **Authentisierungsmodus** den Eintrag **PIN und Authentisierungsgerät**.

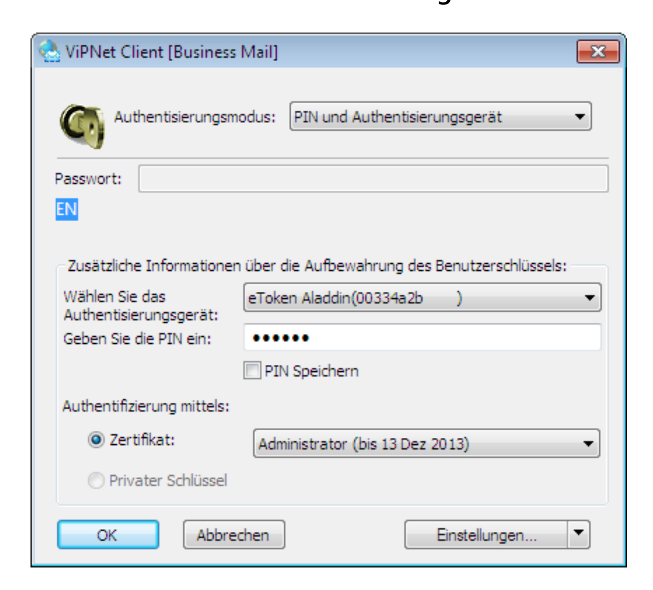


Abbildung 6. Authentisierungsmodus „PIN und Authentisierungsgerät“

2 Schließen Sie das externe Gerät an.

3 Wenn nötig, wählen Sie Ihren Benutzernamen in der Liste darunter aus und geben Sie Ihr Passwort im Feld **Passwort** ein. Ob die Eingabe eines Passworts erforderlich ist, hängt vom Typ des verwendeten externen Geräts ab (s. Abbildung auf S. 27).

4 Wählen Sie in Liste **Authentisierungsgerät** das externe Gerät aus, auf dem sich Ihr privater Schlüssel oder das Zertifikat des privaten Signaturschlüssels befindet.

5 Wenn nötig, geben Sie eine PIN ein. Ob die Eingabe einer PIN erforderlich ist, hängt vom Typ des verwendeten externen Geräts ab. Damit die eingegebene PIN gemerkt wird und bei nachfolgenden Anmeldungen nicht mehr angegeben werden muss, aktivieren Sie das entsprechende Kontrollkästchen.

6 Wählen Sie in Gruppe **Authentifizierung mittels eine** der folgenden Optionen aus:

- **Zertifikat**: um die Authentifizierung mit Hilfe eines Zertifikats, das auf dem benutzten Gerät gespeichert ist, durchzuführen. Wählen Sie das benötigte Zertifikat aus der Liste der Zertifikate, die auf dem Gerät zu finden sind.



Hinweis. Für die Authentifizierung mit Hilfe eines Zertifikats sollten folgende Bedingungen erfüllt sein:

- Der externe Datenträger unterstützt den PKCS#11-Standard.
- Das Zertifikat entspricht dem RSA-Standard.
- Das Zertifikat sollte gültig sein (die Gültigkeitsdauer des Zertifikats sollte nicht abgelaufen sein).
- Das Zertifikat sollte nicht gesperrt sein.
- Die Zertifikatanwendung sollte „Echtheitsüberprüfung des Clients“ lauten. Der Anwendungszweck des Zertifikats wird im Fenster **Zertifikat**, in der Registerkarte **Eigenschaften**, im Feld **Erweiterte Schlüsselverwendung** angezeigt.
- Das Herausgeber-Zertifikat sollte im Systemspeicher **Vertrauenswürdige Stammzertifizierungsstellen** installiert sein.
- Im Container auf dem Gerät befindet sich ein privater Schlüssel, dem das benutzte Zertifikat entspricht.

- **Privater Schlüssel**: wenn Sie die Anmeldung mit Hilfe Ihres privaten Schlüssels durchführen möchten (der private Schlüssel ist Bestandteil der Benutzerschlüssel und wird auf dem verwendeten Gerät gespeichert).

7 Klicken Sie auf **OK**.

Benutzeroberfläche von ViPNet Business Mail

Die Benutzeroberfläche des Programms ViPNet Business Mail ist in der folgenden Abbildung dargestellt:

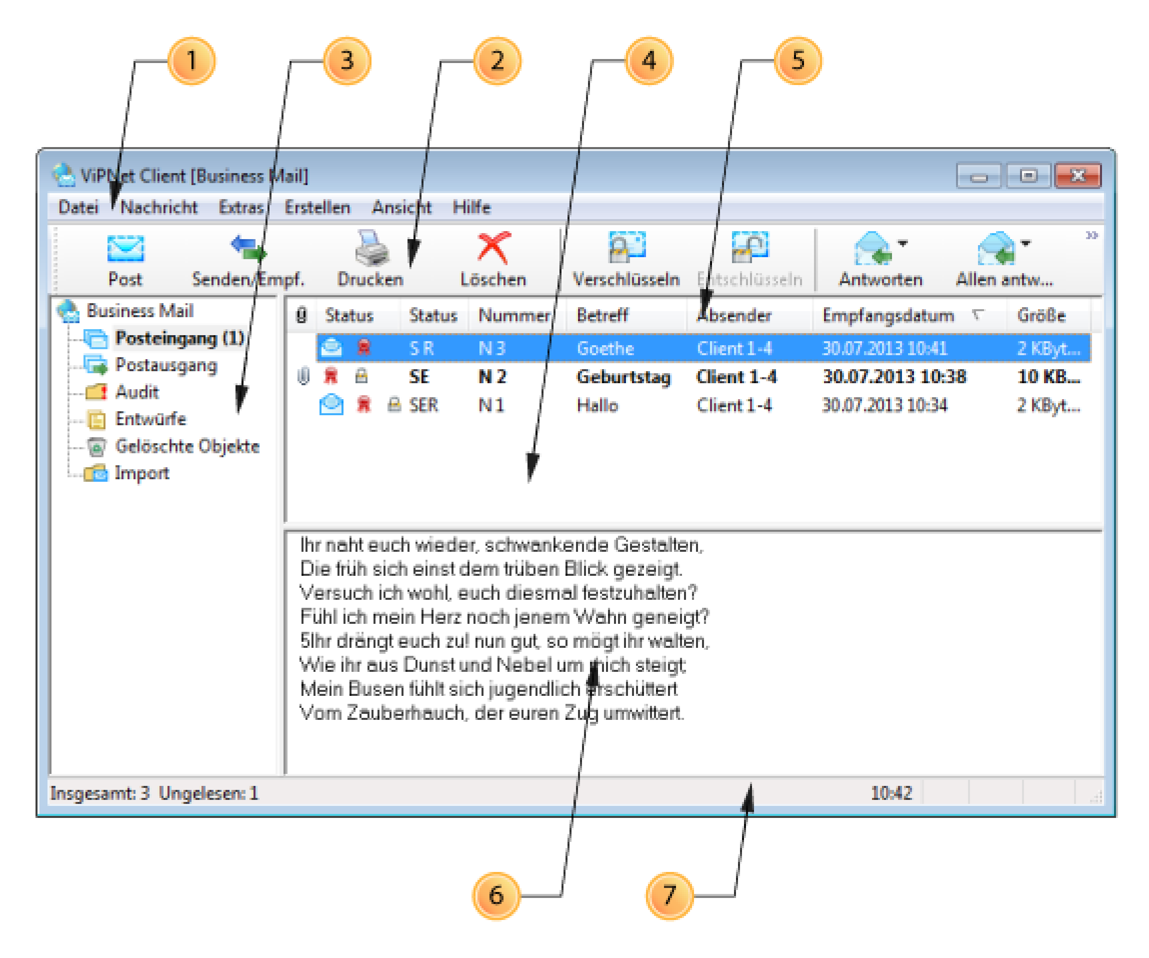


Abbildung 7. Benutzeroberfläche von ViPNet Business Mail

Die Zahlen in der Abbildung kennzeichnen folgende Elemente:

1 Das Hauptmenü des Programms.

2 Die Symbolleiste. Wählen Sie im Menü **Ansicht** den Eintrag **Symbolleiste** und klicken dann auf **Symbolleiste anpassen**, um in der Symbolleiste Schaltflächen hinzuzufügen oder zu entfernen.

3 Der Ordnerbereich. In diesem Bereich wird die Ordnerhierarchie des Programms ViPNet Business Mail abgebildet.

Wenn ein Ordner ungelesene Nachrichten enthält, wird der Ordnername in fetter Schrift dargestellt und die Anzahl der ungelesenen Nachrichten wird in Klammern neben dem Namen des Ordners angezeigt. Wenn ein Ordner weitere Unterordner enthält, die ungelesene Nachrichten enthalten, werden neben dem Ordnernamen in Klammern zwei Zahlen angezeigt: die Anzahl der ungelesenen Nachrichten im Ordner und die Gesamtanzahl der ungelesenen Nachrichten in allen Unterordnern

4 Die Nachrichtenliste. Hier wird die Liste aller Nachrichten in dem Ordner angezeigt, der im Ordnerbereich (**3**) ausgewählt ist.

Wenn Sie die Liste der im Ordner enthaltenen Nachrichten im HTML-Format anzeigen möchten, klicken Sie in der Nachrichtenliste mit der rechten Maustaste auf eine beliebige Spaltenüberschrift und wählen im Kontextmenü den Punkt **Als HTML ansehen**.

5 Die Spalten der Nachrichtenliste (**4**).

Klicken Sie auf eine Spaltenüberschrift, um die Nachrichtenliste nach dieser Spalte zu sortieren. Mit Hilfe des Kontextmenüs können Spalten hinzugefügt oder entfernt werden.

In der Spalte **Status** werden die Statuscodes der Nachricht angezeigt. Eine Beschreibung der Symbole und Statuscodes ist in der nachfolgenden Tabelle enthalten:

Tabelle 3. Nachrichtenattribute

Symbol	Attribut	Status
	E	Die Nachricht und alle Anhänge sind verschlüsselt.
	S	Alle Bestandteile der Nachricht (Text und Anhänge) sind signiert, alle Signaturen sind gültig.
	s	Nicht alle Bestandteile der Nachricht sind signiert, vorhandene Signaturen sind gültig.
	F	Alle Bestandteile der Nachricht sind signiert, aber mindestens eine Signatur ist ungültig.
	f	Nicht alle Bestandteile der Nachricht sind signiert, mindestens eine Signatur ist ungülPtig.
	P	Die Nachricht ist für alle Empfänger verpackt, aber noch nicht versendet.
	p	Die Nachricht ist für einige (nicht alle) Empfänger verpackt, aber noch nicht versendet.
	W	Die Nachricht wurde an alle Empfänger versendet, aber noch nicht empfangen worden.
	w	Die Nachricht wurde an einige (nicht alle) Empfänger versendet, aber noch nicht empfangen worden.
	D	Die Nachricht wurde an alle Empfänger zugestellt, wurde aber noch nicht gelesen.
	d	Die Nachricht wurde an einige Empfänger zugestellt, jedoch nicht an alle.
	R	Im Ordner **Postausgang**: die Nachricht wurde von allen Empfängern gelesen. Im Ordner **Posteingang**: der Nachrichtentext und alle Anhänge wurden gelesen.
	r	Ordner **Postausgang**: die Nachricht wurde von einigen Empfängern gelesen, aber noch nicht von allen. Ordner **Posteingang**: der Nachrichtentext wurde gelesen, jedoch nicht alle Anhänge.
!	!	Die Nachricht kann nicht versendet werden. Diese Situation kann dann auftreten, wenn der Client, an den die Nachricht gesendet wurde, vom Kommunikationsserver getrennt oder aus dem Netzwerk entfernt wurde.



Hinweis. Der Nachrichtentext gilt als gelesen, wenn die Nachricht in einem separaten Fenster geöffnet wurde. Nach dem Beantworten der Nachricht gilt der Text dieser Nachricht als gelesen.

Die Anlage gilt als eingesehen, wenn sie angezeigt oder abgespeichert wurde.

Beim Weiterleiten oder beim Speichern einer Nachricht auf dem Laufwerk gelten der Nachrichtentext sowie alle Anhänge als gelesen.

6 Der Vorschaubereich. In diesem Bereich wird der Brieftext der in der Liste (**4**) ausgewählten Nachricht eingeblendet.

7 Die Statusleiste. In der Statuszeile wird die Gesamtanzahl der Nachrichten im ausgewählten Ordner sowie die Anzahl der ungelesenen (im Ordner **Posteingang**) bzw. nicht zugestellten (im Ordner **Postausgang**) Nachrichten angezeigt.

Die Anzahl von Nachrichten eines bestimmten Typs wird als Summe zweier Zahlen angezeigt: die Anzahl der Nachrichten dieses Typs im ausgewählten Ordner und die Gesamtanzahl der Nachrichten dieses Typs in allen Unterordnern.

Wählen Sie im Menü **Ansicht** den Punkt **Statusleiste**, um die Statusleiste ein- oder auszublenden.

Speichern der Nachrichten mit Hilfe der Ordner

Die gespeicherten Nachrichten können in „Business Mail" mit Hilfe der Ordnerhierarchie organisiert werden. Die Ordner werden im Navigationsbereich in der Navigationsleiste des Hauptfensters eingeblendet (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31).

Die Ordner in „Business Mail" können in zwei Kategorien eingeteilt werden:

- Vordefinierte Ordner – werden automatisch von „Business Mail" erzeugt und können nicht umbenannt oder entfernt werden.
- Benutzerdefinierte Ordner – werden vom Benutzer erstellt, können umbenannt oder gelöscht werden.

Die bei der Arbeit mit Ordnern möglichen Aktionen sind in den nachfolgenden Abschnitten beschrieben.

Vordefinierte Ordner

Die Aktionsmöglichkeiten bei vordefinierten Ordnern sind in „Business Mail" eingeschränkt. Vordefinierte Ordner und ihre Besonderheiten sind nachfolgend aufgelistet:

- **Posteingang** – Ordner, in dem standardmäßig die empfangenen Nachrichten (s. Nachrichten und Anhänge im separaten Fenster anzeigen auf S. 50) abgelegt werden.
- **Posteingang > ACK (Bestätigung der Datenübertragung)** – Ordner, in dem Empfangs- und Lesebestätigungen (s. Anfrage der Empfangs– und Lesebestätigungen als separate Nachricht auf S. 44) als separate Nachrichten abgelegt werden.

  Dieser Ordner wird beim Empfang der ersten Bestätigung automatisch erzeugt, standardmäßig fehlt er.
- **Postausgang** – Ordner, in dem erstellte Nachrichten (s. Verfassen der Nachricht auf S. 42) abgelegt werden.
- **Postausgang > ACK (Bestätigung der Datenübertragung)** – Ordner, in dem Übermittlungsbestätigungen als separate Nachrichten abgelegt werden.

  Dieser Ordner wird beim Versenden der ersten Bestätigung automatisch erzeugt, standardmäßig fehlt er.
- **Gelöschte Objekte** – Ordner, in dem gelöschte Nachrichten (s. Nachrichten löschen auf S. 59) abgelegt werden.

  Im Ordner **Gelöschte Objekte** können keine Unterordner erzeugt oder umbenannt werden.
- **Audit** – Ordner, der Informationen über Nachrichten enthält, die aus dem Ordner **Gelöschte Objekte** entfernt wurden.

Im Ordner **Audit** können keine Unterordner erzeugt oder umbenannt werden. Das Löschen von Ordnern und Nachrichten im Ordner **Audit** ist nur beim Arbeiten im Administrator-Modus (s. Arbeiten mit Administratorrechten auf S. 114) möglich.

- **Entwürfe** – Ordner, in dem Nachrichtenentwürfe (s. Nachrichtenvorlagen erstellen und verwenden auf S. 46) abgelegt werden.
- **Import** – Ordner, in dem importierte Nachrichten (s. Nachrichten exportieren und importieren auf S. 56) abgelegt werden.

Benutzerdefinierte Ordner

Verwenden von Ordnern hilft Ihnen, die Postdatenbank von „Business Mail" zu organisieren.

Um einen neuen Ordner zu erstellen:

1 Wählen Sie in der Ordnerübersicht (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) ein Verzeichnis, innerhalb von dem ein neuer Ordner erzeugt werden soll (dies kann auch das Stammverzeichnis **Business Mail** sein), und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie im Kontextmenü den Eintrag **Neuen Ordner erstellen**.
   - Wählen Sie in Menü **Datei** den Eintrag **Ordner** und klicken Sie dann auf **Neuer Ordner**.

   Es wird das Fenster **Neuen Ordner erzeugen** geöffnet.

2 Geben Sie im Fenster **Neuen Ordner erzeugen** den Namen des neuen Ordners ein und klicken Sie auf **OK**. In der Ordnerübersicht erscheint das neue Verzeichnis mit dem angegebenen Namen.



Hinweis. Innerhalb eines Verzeichnisses können keine zwei Ordner mit dem gleichen Namen erzeugt werden. In **Gelöschte Objekte** und **Audit** (s. Vordefinierte Ordner auf S. 34) ist das Erzeugen neuer Unterordner nicht möglich.

Um einen Ordner umzubenennen:

1 Wählen Sie in der Ordnerübersicht (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) den Ordner, der umbenannt werden soll, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf den Ordnernamen.
   - Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie im Kontextmenü den Eintrag **Ordner umbenennen**.

   Anstelle des Ordnernamens erscheint ein Eingabefeld.

2 Geben Sie den neuen Namen ein. Drücken Sie anschließend die **Eingabetaste** oder klicken Sie in einen Bereich außerhalb des Eingabefelds.



Hinweis. Innerhalb eines Verzeichnisses können keine zwei Ordner mit dem gleichen Namen erzeugt werden. Vordefinierte Ordner (auf S. 34) können nicht umbenannt werden.

Um einen Ordner zu verschieben, klicken Sie auf den Ordner und ziehen Sie ihn mit der Maus in den Zielordner. Folgende Verschiebungen können nicht vorgenommen werden:

- aus dem Ordner **Posteingang** und **Gelöschte Objekte** > **Posteingang** in den Ordner **Postausgang**;
- aus beliebigen Ordnern mit Ausnahme von **Gelöschte Objekte** > **Posteingang** in den Ordner **Posteingang**;
- nach **Entwürfe**, **Gelöschte Objekte** und **Audit**;
- zwischen zwei Unterordnern von **Gelöschte Objekte** oder **Audit**.

Um Ordnerinhalt zu leeren:

1. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie im Kontextmenü den Eintrag **Ordner leeren**.
2. Im Dialogfeld zur Bestätigung der Aktion klicken Sie auf **Ja**.

   Alle Nachrichten innerhalb des Ordners werden entfernt (s. Nachrichten löschen auf S. 59).

Um einen Ordner zu löschen:

1. Wählen Sie den Ordner, der gelöscht werden soll, und führen Sie einen der folgenden Schritte aus:
   - Drücken Sie die **Entf**–Taste.
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen** ✗.
2. Im Dialogfeld zur Bestätigung der Aktion klicken Sie auf **Ja**.

   Der gewählte Ordner wird mitsamt allen Unterordnern in **Gelöschte Objekte** verschoben. Dabei wird im Ordner **Gelöschte Objekte** automatisch eine Ordnerhierarchie erzeugt, die mit der ursprünglichen vollständig übereinstimmt. Ein Beispiel: in **Postausgang** > **Ordner–1** befindet sich **Ordner–2**. Beim Löschen von **Ordner–2** wird dieser mit seinem kompletten Inhalt in **Gelöschte Objekte** > **Posteingang** > **Ordner–1** verschoben.

   Beim Entfernen des Ordners aus **Gelöschte Objekte** wird der Ordner auf genau die gleiche Weise in den Ordner **Audit** verschoben. Die im Ordner abgelegten Nachrichten werden dabei durch Einträge ersetzt, die die Löschzeit sowie den Namen des Benutzers, der den Vorgang ausgelöst hat, enthalten. Im Ordner **Audit** können Ordner nur vom Netzwerkknoten-Administrator (s. Arbeiten mit Administratorrechten auf S. 114) gelöscht werden.

Das Adressbuch

Das Adressbuch stellt eine Liste der Empfänger dar, an die Nachrichten versendet werden können. Diese Liste kann nicht vom Netzwerkknoten–Benutzer geändert werden, da sie durch Beziehungen definiert ist, die vom ViPNet Netzwerk Administrator im ViPNet Network Control Center oder ViPNet Network Manager für den betreffenden Netzwerkknoten festgelegt wurden.

Klicken Sie im ViPNet Business Mail Hauptfenster im Menü **Extras** auf **Adressbuch**, um das Adressbuch zu öffnen. Es wird das Fenster **Adressbuch** eingeblendet.

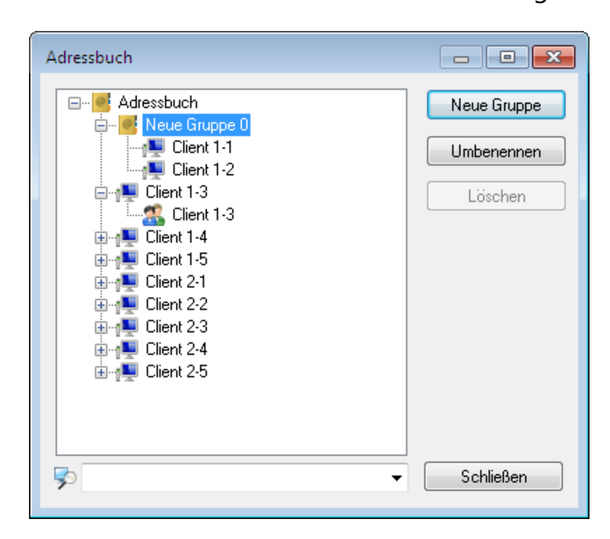


Abbildung 8. Adressbuch von „Business Mail“

Das Adressbuch wird für die Auswahl der Empfänger beim Erstellen einer Nachricht (s. Neue Nachricht erstellen und versenden auf S. 40) verwendet. Nachrichten können an Netzwerkknoten, Arbeitsgruppen oder bestimmte Benutzer des ViPNet–Netzwerks adressiert werden. Auf diese Weise existieren in „Business Mail“ drei Stufen der Adressierung (s. Ebenen der Adressierung auf S. 37).

Aus praktischen Gründen können die Clients im Adressbuch in Gruppen unterteilt werden (s. Empfängergruppen auf S. 38).

Ebenen der Adressierung

Jedem Client, der über eine Verbindung mit dem aktuellen Client verfügt, entsprechen im Adressbuch von „Business Mail“ (s. Abbildung auf S. 37) drei Ebenen der Adressierung:

1. Netzwerkknoten. Diese Ebene der Adressierung beinhaltet alle Benutzer eines Netzwerkknotens. Eine verschlüsselte Nachricht, die an einen Knoten adressiert ist, kann von allen Benutzern dieses Knotens gelesen werden.

2. Arbeitsgruppe. Diese Ebene der Adressierung entspricht einer Gruppe von Benutzern, die auf dem Netzwerkknoten registriert sind. Eine verschlüsselte Nachricht, die an eine Arbeitsgruppe adressiert ist, kann nur von Mitgliedern dieser Gruppe gelesen werden.

3 Benutzer. Diese Ebene der Adressierung entspricht einem bestimmten Benutzer des Clients. Eine Nachricht, die an einen Benutzer adressiert ist, kann von allen Mitgliedern seiner Arbeitsgruppe gelesen werden. Dadurch kann diese Ebene der Adressierung nicht für Zugriffsbeschränkungen für verschlüsselte Nachrichten verwendet werden, sie dient nur zur Bestimmung des Empfängers.



Hinweis. Wenn der Benutzer das einzige Mitglied seiner Arbeitsgruppe ist, und sein Name mit dem Gruppennamen übereinstimmt, wird im Adressbuch von Programm ViPNet Business Mail nur die Gruppe aufgeführt, der Benutzer erscheint dort nicht mehr.

Empfängergruppen

Standardmäßig ist im Adressbuch von „Business Mail" eine Empfängergruppe angelegt, deren Name **Adressbuch der geschützten Firmenpost** lautet. Diese Gruppe kann nicht umbenannt oder entfernt werden.

Führen Sie die folgenden Schritte aus, um eine neue Gruppe zu erstellen:

1 Klicken Sie im ViPNet Business Mail Hauptfenster im Menü Extras auf den Eintrag Adressbuch oder klicken Sie im Fenster zur Erfassung einer neuen Nachricht (s. Neue Nachricht erstellen und versenden auf S. 40) auf die Schaltfläche **Empfänger** .

2 Im Fenster **Adressbuch** (s. Abbildung auf S. 37) wählen Sie die Clientgruppe, innerhalb welcher eine neue Gruppe angelegt werden soll.

3 Klicken Sie auf die Schaltfläche **Gruppe hinzufügen**. Im Adressbuch werden ein neuer Ordner und ein Eingabefeld für den Ordnernamen eingeblendet.

4 Geben Sie den Namen der neuen Gruppe ein und drücken Sie die **Eingabetaste**.

5 Um einen Client in die neue Gruppe aufzunehmen, klicken Sie auf den Client, seine Arbeitsgruppe oder einen Benutzer und ziehen Sie ihn mit der Maus in die Gruppe.

So benennen Sie eine Gruppe um:

1 Wählen Sie die Gruppe im Fenster **Adressbuch** aus.

2 Klicken Sie auf die Schaltfläche **Umbenennen**. Anstatt des Gruppennamens erscheint ein Eingabefeld.

3 Geben Sie den neuen Namen ein und drücken Sie anschließend entweder die **Eingabetaste** oder klicken Sie in einen Bereich außerhalb des Eingabefelds.

So löschen Sie eine Gruppe:

1 Wenn in einer Gruppe, die gelöscht werden soll, Clients enthalten sind, dann verschieben Sie diese zunächst in andere Gruppen. Eine Gruppe, die Clients enthält, kann nicht gelöscht werden.

2 Wählen Sie die Gruppe in der Liste aus.

3 Klicken Sie auf die Schaltfläche **Löschen**. Die Gruppe wird gelöscht.

3

Arbeiten mit Nachrichten

Neue Nachricht erstellen und versenden

Fenster zum Anzeigen und Verfassen von Nachrichten

Der Aufbau des Fensters, in dem neue Nachricht verfasst (s. Verfassen der Nachricht auf S. 42) sowie versendete und empfangene Nachrichten angezeigt werden (s. Nachrichten und Anhänge im separaten Fenster anzeigen auf S. 50), ist in der folgenden Abbildung dargestellt:

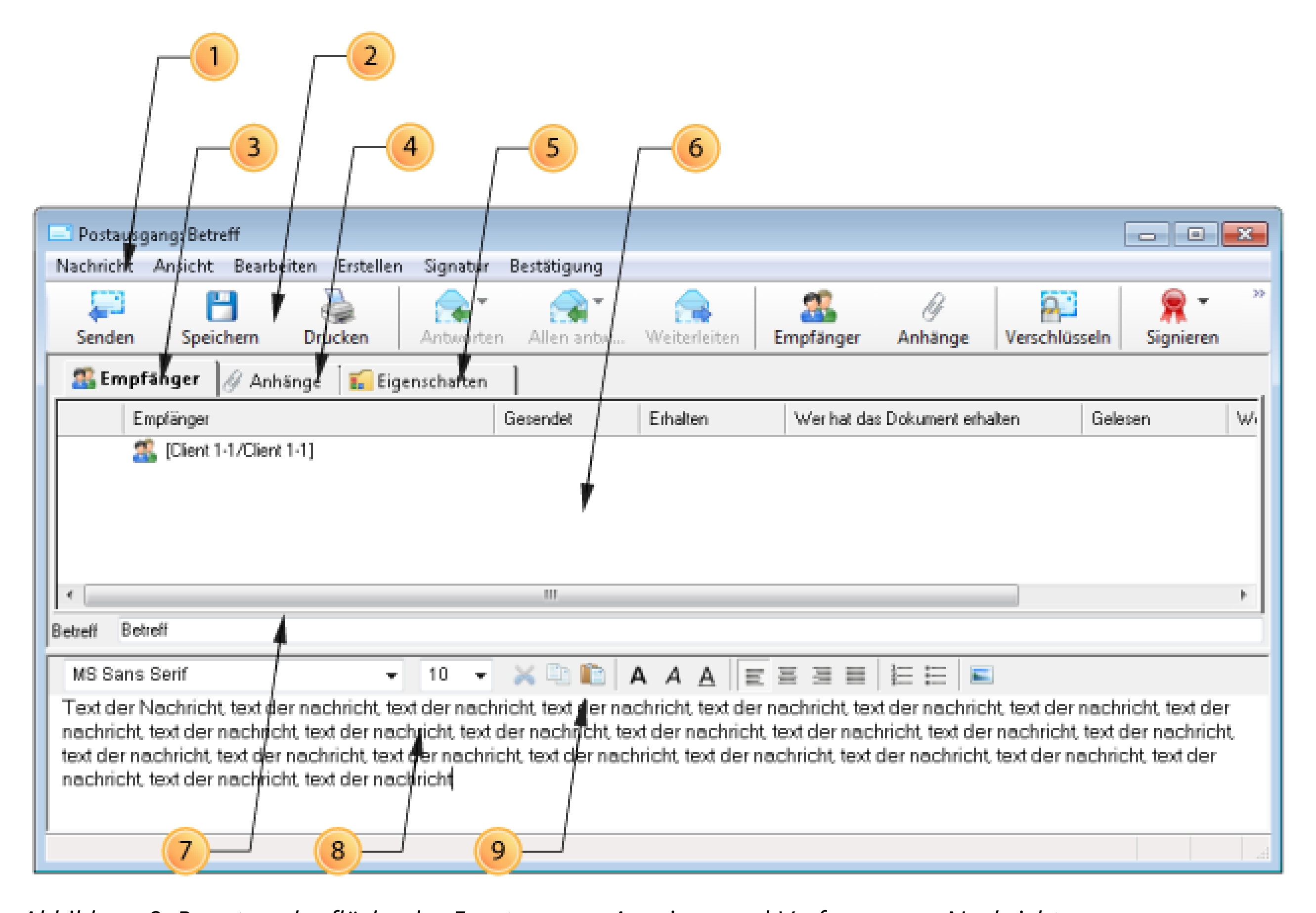


Abbildung 9. Benutzeroberfläche des Fensters zum Anzeigen und Verfassen von Nachrichten

Die Zahlen in der Abbildung kennzeichnen die folgenden Elemente:

1 Das Hauptmenü.

2 Die Symbolleiste. Wählen Sie im Menü **Ansicht** den Eintrag **Symbolleiste** und klicken auf **Symbolleiste anpassen**, um in der Symbolleiste Schaltflächen hinzuzufügen oder zu entfernen.

3 Die Registerkarte **Empfänger**. In dieser Registerkarte werden die Empfänger der Nachricht aufgeführt. Wenn eine bereits versendete oder empfangene Nachricht geöffnet wird, werden hier

zusätzlich die Informationen über die Sende– und Empfangszeit, den Nachrichtenempfänger u.s.w. eingeblendet.

4 Die Registerkarte **Anhänge**. In dieser Registerkarte werden alle in der Nachricht enthaltenen Dateianhänge angezeigt.

5 Die Registerkarte **Eigenschaften**. Diese Registerkarte enthält Informationen über die Registrierungsnummer, das Erstelldatum und den Absender der Nachricht sowie die Zeit der letzten Gültigkeitsprüfung der digitalen Signatur (soweit vorhanden).

6 Der Bereich für die Darstellung des Inhalts der Registerkarten **Empfänger**, **Anhänge** und **Eigenschaften**.

7 Die Betreffzeile. In diesem Feld wird der Betreff der Nachricht angezeigt.

8 In diesem Bereich wird der Nachrichtentext angezeigt.

9 Textformatierungsleiste. Mit Hilfe dieser Leiste können beim Erstellen einer Nachricht die Schriftart, die Schriftgröße und der Schriftschnitt geändert, ein Bild, eine Liste in den Text eingefügt werden usw. Der Bedeutung der wichtigsten Schaftflächen der Formatierungsleiste sind in der Tabelle unten beschrieben.

Tabelle 4. Schaltflächen der Formatierungsleiste

Schaltfläche	Aktion	Tastenkombination
	Fett formatieren	**Strg+B**
	Kursiv formatieren	**Strg+I**
	Unterstreichen	**Strg+U**
	Linksbündig ausrichten (standardmäßig)	**Strg+L**
	Zentrieren	**Strg+E**
	Rechtsbündig ausrichten	**Strg+R**
	Im Blocksatz ausrichten	**Strg+J**
	Eine numerische Liste erstellen	—
	Eine Aufzählung erstellen	—
	Bild einfügen	—



Hinweis. Standardmäßig wird die Formatierungsleiste nicht angezeigt und Nachrichten werden ohne Formatierung erstellt. Möchten Sie den Nachrichtentext formatieren, aktivieren Sie die Formatierung in den Einstellungen der allgemeinen Parameter (s. Allgemeine Parameter einstellen auf S. 103).

Verfassen der Nachricht

Führen Sie die folgenden Schritte aus, um eine Nachricht zu verfassen:

1. Klicken Sie im Hauptfenster von ViPNet Business Mail in der Symbolleiste auf die Schaltfläche **Post** . Es wird das Fenster zum Verfassen einer neuen Nachricht geöffnet (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40).
2. Geben Sie im Feld **Betreff** den Betreff der Nachricht ein.
3. Geben Sie im unteren Bereich den Text der Nachricht ein.
4. Konfigurieren Sie bei Bedarf das Format des Nachrichtentextes mit Hilfe der Formatierungsleiste. Wird die Formatierungsleiste im Fenster zum Verfassen von Nachrichten nicht angezeigt, aktivieren Sie die Formatierung in den Einstellungen der allgemeinen Parameter (s. Allgemeine Parameter einstellen auf S. 103).



Hinweis. Versenden Sie eine Nachricht mit Formatierung an einen Empfänger, der eine frühere Textformatierung nicht unterstützende Version von ViPNet Business Mail verwendet, erhält dieser Empfänger den Text Ihrer Nachricht als Anhang im RTF-Format (Rich Text Format) und kann ihn mit Hilfe eines Textverarbeitungsprogramms lesen, z.B. Microsoft Office Word oder Microsoft WordPad.

5. Wenn Anhänge hinzugefügt werden sollen:
   - Führen Sie einen der folgenden Schritte aus:
     - Ziehen Sie die Dateien mit der Maus in das Nachrichtenfenster.
     - Klicken Sie in der Symbolleiste auf die Schaltfläche **Anhänge** . Wählen Sie im Fenster Öffnen eine oder mehrere Dateien aus.

     Für jede Datei wird das Fenster **Geben Sie den Anhangnamen ein** eingeblendet. Standartmäßig stimmt der Anhangnahmen mit dem Dateinamen überein.



Hinweis. Die Beschreibung des Anhangs sollte nicht mehr als 56 Symbole enthalten.

   - Klicken Sie auf **Alle hinzufügen**, um alle Dateien unter Beibehaltung der Anhangnamen anzuhängen. Geben Sie für jeden Anhang einen Namen ein und klicken Sie auf **Hinzufügen**, um die Anhangnamen zu ändern.

     Die gewählten Dateien werden an die Nachricht angehängt.



Hinweis. Die Gesamtgröße der hinzugefügten Anhänge darf nicht 2 GB überschreiten.

Zum Entfernen der Anhänge:

- Öffnen Sie im Nachrichtenfenster die Registerkarte **Anhänge**.
- Wählen Sie die Datei aus, die entfernt werden soll, und drücken die **Entf**–Taste.

6. Wenn die Nachricht verschlüsselt werden soll, klicken Sie in der Symbolleiste auf die Schaltfläche **Verschlüsseln** . Wenn die Nachricht digital signiert werden soll (s. Digitale Signatur und Verschlüsselung auf S. 65), klicken Sie auf die Schaltfläche **Signieren** .

7. So bestimmen Sie die Empfänger der Nachricht:

   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Empfänger** . Es wird das Fenster **Addressbuch** geöffnet (s. Das Adressbuch auf S. 37).

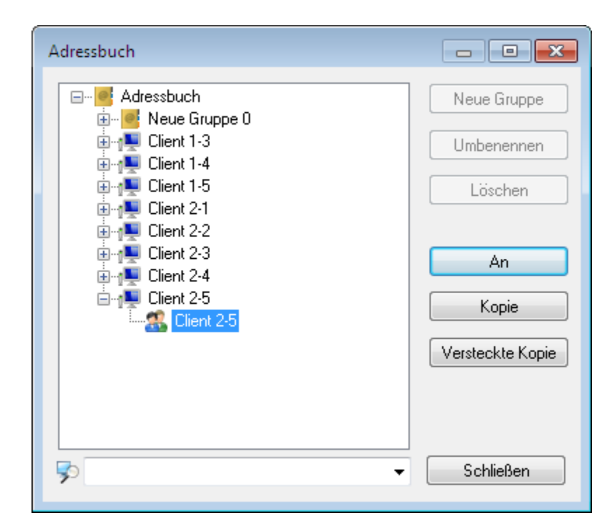
   

   Abbildung 10. Empfänger auswählen

   - Wählen Sie im Fenster **Adressbuch** einen oder mehrere Emfänger aus (s. Ebenen der Adressierung auf S. 37). Zum Filtern der Empfängerliste geben Sie in der Suchzeile im unteren Fensterbereich einen Teil des benötigten Empfängernamens ein.

     Nach Auswahl eines oder mehrerer Empfänger führen Sie eine der folgenden Aktionen aus:

     - Klicken Sie auf die Schaltfläche **An**, um die Nachricht an die gewählten Empfänger zu adressieren.
     - Klicken Sie auf **Kopie**, um eine Kopie der Nachricht an die gewählten Empfänger zu versenden.
     - Klicken Sie auf **Versteckte Kopie**, um eine blinde Kopie der Nachricht an die gewählten Empfänger zu versenden.

   - Wiederholen Sie die oben angeführten Schritte, um alle benötigten Empfänger hinzuzufügen. Klicken Sie dann im Fenster **Adressbuch** auf die Schaltfläche **Schließen**.

   Wenn Sie einen Empfänger wieder entfernen möchten, wählen Sie diesen in der Registerkarte **Empfänger** aus (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40) und drücken Sie die **Entf**–Taste.

8. Für jeden Empfänger kann eine Notiz verfasst werden – eine kurze Anmerkung von nicht mehr als 245 Zeichen. So erstellen Sie eine Notiz:

   - Doppelklicken Sie auf den Empfängernamen und geben Sie im Fenster **Notiz** den Text ein.

- Klicken Sie auf **OK**. Links vom Empfängernamen wird das Symbol eingeblendet.

9 Sobald Sie mit dem Verfassen einer Nachricht fertig sind, führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern** oder schließen das Nachrichtenfenster und klicken dann im Dialogfeld zum Speichern von Änderungen auf **Ja**, um die Nachricht im Ordner **Postausgang** zu speichern.
- Klicken Sie in der Symbolleiste auf **Senden**, um die Nachricht zu versenden.



Hinweis. Der Statuscode der versendeten Nachricht kann im Ordner **Postausgang** in der Spalte **Status** (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) abgelesen werden. Es kann auch eine Empfangsbestätigung (s. Anfrage der Empfangs– und Lesebestätigungen als separate Nachricht auf S. 44) angefordert werden.

Anfrage der Empfangs– und Lesebestätigungen als separate Nachricht

Beim Versenden von Nachrichten kann in „Business Mail" eine Lese– oder Empfangsbestätigung angefordert werden. So fordern Sie eine Bestätigung an:

1 Führen Sie die im Abschnitt Nachricht verfassen (s. Verfassen der Nachricht auf S. 42) beschriebenen Schritte aus.

2 Wählen Sie vor dem Absenden der Nachricht im Menü **Bestätigung** den Eintrag **Empfangsbestätigung anfragen** oder klicken Sie in der Symbolleiste auf die Schaltfläche **Bestätigung** .

3 Klicken Sie auf **Senden**, um die E–Mail zu versenden.

Nach dem Erhalt der Nachricht durch den Empfänger wird automatisch eine Empfangsbestätigung an den Absender versendet, nach dem Lesen der Nachricht – eine Lesebestätigung. Die Bestätigungen der Datenübertragung stellen normale „Business Mail" Nachrichten dar. Der Betreff stimmt mit dem Betreff der Originalnachricht überein, es wird aber zusätzlich das Präfix „AD:" (bei Empfangsbestätigungen) oder „AR:" (bei Lesebestätigungen) in der Betreffzeile hinzugefügt. Wenn die Originalnachricht verschlüsselt ist, wird die Bestätigung ebenfalls verschlüsselt.

In „Business Mail" werden ausgehende Bestätigungen auf dem Client des Empfängers im Ordner **Postausgang** > **ACK (Bestätigung der Datenübertragung)** abgelegt. Auf dem Client des Absenders eingehende Bestätigungen werden im Ordner **Posteingang** > **ACK (Bestätigung der Datenübertragung)** gespeichert. Diese Unterordner werden beim Empfang oder Versand der ersten Bestätigung automatisch erzeugt und können nicht umbenannt oder entfernt werden. Der Statuscode einer Bestätigung kann wie der Statuscode einer normalen Nachricht in der Spalte **Status** abgelesen werden.

Eine Empfangsbestätigung enthält folgende Informationen:

- Datum und Uhrzeit des Nachrichtenerhalts.

- Betreff der Nachricht.
- Name des Absenders und Ergebnis der Gültigkeitsprüfung der digitalen Signatur.
- Registrierungsnummer der Nachricht.
- Ergebnis der Gültigkeitsprüfung der digitalen Signatur für den signierten Nachrichtentext und für alle signierten Anhänge.
- Prüfsummen der digitalen Signatur für den signierten Nachrichtentext und für alle signierten Anhänge.

Nachricht als Anhang versenden

Führen Sie folgende Schritte aus, um in „Business Mail" eine Nachricht als Anhang zu versenden:

1 Wählen Sie in der Navigationsleiste des ViPNet Business Mail Hauptfensters (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) den Ordner mit Nachrichten, die als Anhang versendet werden sollen.

2 Wählen Sie eine oder mehrere E–Mails in der Nachrichtenliste aus.

3 Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen Sie im Kontextmenü den Eintrag **Als Anhang versenden**.
   - Klicken Sie im Menü **Nachricht** auf **Als Anhang versenden**.

   Es wird das Fenster zum Verfassen einer neuen Nachricht geöffnet. Für jede ausgewählte Nachricht, die als Anhang versendet werden soll, wird separat das Fenster **Anhangnamen eingeben** geöffnet.

4 Klicken Sie auf **Alle hinzufügen**, um alle Nachrichten als Dateien unter Beibehaltung ihrer Namen anzuhängen. Um die Dateinamen zu ändern, geben Sie für jeden Anhang einen Namen ein und klicken Sie auf **Hinzufügen**.

   Die gewählten Nachrichten werden als Anhänge hinzugefügt.

5 Schließen Sie das Verfassen der Nachricht ab und versenden die Nachricht anschließend wie im Abschnitt Nachricht verfassen (s. Verfassen der Nachricht auf S. 42) beschrieben.

Nachrichtenvorlagen erstellen und verwenden

Für den häufigen Versand gleichartiger Nachrichten ist es praktischer, Vorlagen zu verwenden. Vorlagen werden in „Business Mail" im Ordner **Entwürfe** gespeichert. Eine Vorlage kann auf zwei Arten erstellt werden:

1 Vorlage auf Basis einer vorhandenen Nachricht erstellen. Dazu führen Sie die folgenden Schritte aus:

   1.1 Wählen Sie die Nachricht, die als Basis für die Vorlage dienen soll.

   1.2 Verschieben Sie die Nachricht (s. Nachrichten in andere Programmsordner verschieben auf S. 58) in den Ordner **Entwürfe** oder einen Unterordner davon.

   Auf Basis der gewählten Nachricht wird im Ordner **Entwürfe** eine neue Vorlage erstellt, die Nachricht selbst verbleibt dabei im Quellordner.

   Die neu erstellte Vorlage behält alle Eigenschaften der Originalnachricht ausgenommen Registrierungsnummer, digitale Signatur sowie Empfangs–, Lese– und Sendestatuscodes. Als Absender wird der Benutzer angegeben, der die Vorlage erstellt hat.

2 Eine neue Vorlage erstellen. Dazu führen Sie die folgenden Schritte aus:

   2.1 Wählen Sie im Hauptfenster von „Business Mail" im Menü **Erstellen** den Eintrag **Neuer Entwurf**.

   2.2 Es wird das Fenster **Entwurf** geöffnet, das dem Fenster zum Verfassen einer neuen Nachricht entspricht (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40).

   2.3 Geben Sie den Nachrichtentext und den Betreff ein, bestimmen Sie die Empfänger und setzen Sie weitere Parameter wie im Abschnitt Nachricht verfassen (s. Verfassen der Nachricht auf S. 42) beschrieben.

   2.4 Klicken Sie auf **Speichern** .

   Die Entwurf wird im Ordner **Entwürfe** gespeichert. Der neue Entwurf bekommt keine Registrierungsnummer zugewiesen, als Absender wird der Benutzer angegeben, der die Vorlage erstellt hat.

Führen Sie die folgenden Schritte aus, um ein Entwurf zum Verfassen einer neuen Nachricht zu verwenden:

1 Wählen Sie in der Navigationsleiste des Hauptfensters von „Business Mail" den Ordner **Entwürfe** aus (oder einen Unterordner davon, der die benötigte Vorlage enthält).

2 Doppelklicken Sie auf den Entwurf oder wählen Sie diesen in der Liste aus und drücken anschließend die **Eingabetaste**.

3 Klicken Sie im Entwürfe-Fenster in der Symbolleiste auf die Schaltfläche **Kopieren** . Im Ordner **Postausgang** wird eine Nachricht erstellt, die eine Kopie des Entwurfs darstellt.

4 Modifizieren Sie bei Bedarf die erstellte Nachricht (s. Verfassen der Nachricht auf S. 42) und senden diese anschließend ab.

Nachrichten und ihre Eigenschaften im Hauptfenster anzeigen

So zeigen Sie eine Nachricht an:

1. Wählen Sie in der Navigationsleiste des ViPNet Business Mail Hauptfensters (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) den Ordner, in dem sich die Nachricht befindet.



Hinweis. Wenn ein Ordner oder sein Unterordner ungelesene Nachrichten enthält, wird der Ordnername in fetter Schrift hervorgehoben. Die Anzahl der ungelesenen Nachrichten wird neben dem Ordnernamen in Klammern angezeigt

Die im gewählten Ordner enthaltenen ungelesenen Nachrichten werden in der Nachrichtenliste in fetter Schrift dargestellt.

---

2. Wählen Sie die Nachricht in der Liste aus.

   Wenn die Nachricht nicht verschlüsselt ist, wird ihr Text im Nachrichtenbereich eingeblendet. Wenn die Nachricht noch nicht gelesen wurde, gilt sie nach dieser Aktion noch immer als nicht gelesen.

   Wenn die Nachricht verschlüsselt ist, wird im Nachrichtenbereich der Text „Dieser Brief ist verschlüsselt. Öffnen Sie den Brief, um ihn zu lesen." eingeblendet. Führen Sie einen der folgenden Schritte aus, um die verschlüsselte Nachricht zu lesen:

   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Entschlüsseln** . Der Nachrichtentext wird im Lesebereich eingeblendet. Wenn die Nachricht noch nicht gelesen wurde, gilt sie nach dieser Aktion noch immer als nicht gelesen.
   - Öffnen Sie die Nachricht in einem separaten Fenster (s. Nachrichten und Anhänge im separaten Fenster anzeigen auf S. 50).

3. Wenn die Nachricht Anhänge enthält (in der Spalte **Anhang** wird ein Klammersymbol eingeblendet), öffnen Sie die Nachricht in einem separaten Fenster (s. Nachrichten und Anhänge im separaten Fenster anzeigen auf S. 50), um die Anhänge zu sehen.

Im Hauptfenster des Programms sind außerdem folgende Aktionen möglich:

1. Klicken Sie mit der rechten Maustaste auf die Nachricht und wählen Sie im Kontextmenü den Eintrag Als gelesen markieren, um eine noch nicht gelesene Nachricht als gelesen zu markieren. In der Spalte Status wird dabei der Symbol eingeblendet (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31).
2. Klicken Sie mit der rechten Maustaste auf die Nachricht und wählen Sie im Kontextmenü den Eintrag **Als ungelesen markieren**, um eine gelesene Nachricht als nicht gelesen zu markieren. Die Statuscodes der Nachricht werden dabei nicht geändert.
3. Für noch nicht versendete Nachrichten kann die Registrierungsnummer geändert werden (s. Nachrichtenparameter einstellen auf S. 109). So ändern Sie die Nummer:

- Wählen Sie im Ordner **Postausgang** eine noch nicht versendete Nachricht aus.
- Klicken Sie mit der rechten Maustaste auf die Nachricht und wählen Sie im Kontextmenü den Eintrag **Registrierungsnummer ändern**. Es wird das Fenster **Änderung der Registrierungsnummer** eingeblendet.

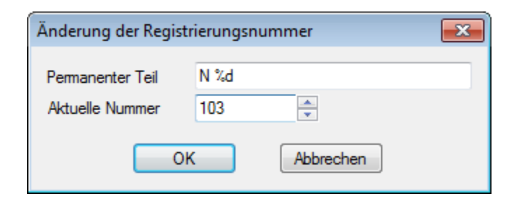


Abbildung 11. Änderung der Registrierungsnummer

- Tragen Sie im Feld **Permanenter Teil** den permanenten Teil der Nummer ein, wenn erforderlich.
- Geben Sie im Feld **Aktuelle Nummer** die Nummer ein, die der Nachricht zugewiesen werden soll. Die eingegebene Nummer kann nicht kleiner sein als die letzte zugewiesene Nummer (wird im Feld standardmäßig eingeblendet) und kann diese um nicht mehr als 100 übersteigen.
- Sobald Sie mit der Eingabe der Registrierungsnummer fertig sind, klicken Sie auf **OK**.

Wenn für eine Nachricht der permanente Teil der Nummer geändert wurde, ändert sich der in den Nachrichteneinstellungen fixierte (s. Nachrichtenparameter einstellen auf S. 109) Wert des permanenten Teils nicht. Wenn die laufende Nummer geändert wurde, ändert sich diese auch in den Programmeinstellungen und wird ab diesem Zeitpunkt als Basis für die fortlaufende Nummerierung benutzt.

4. Zum Versenden einer noch nicht gesendeten Nachricht wählen Sie die Nachricht im Ordner **Postausgang** aus, klicken Sie auf diese mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Senden**.
5. Zum Anzeigen von Details über die Nachricht und ihre Empfänger klicken Sie mit der rechten Maustaste auf die Nachricht und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**. Es wird das Fenster **Eigenschaften der Nachricht** eingeblendet.

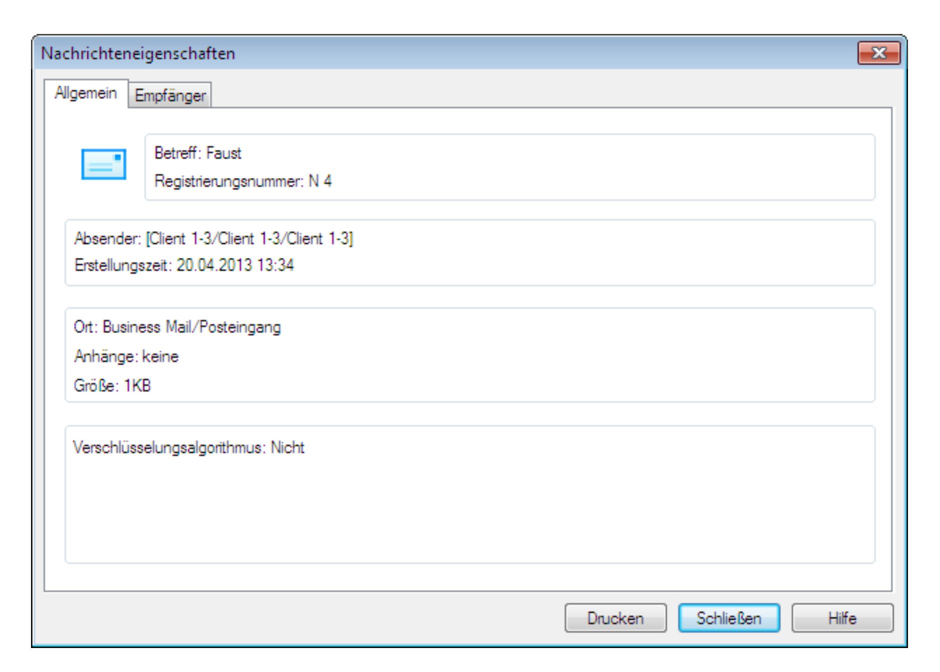


Abbildung 12. Eigenschaften der Nachricht

6 Zum Drucken einer Nachricht wählen Sie die Nachricht aus der Nachrichtenliste aus und klicken auf die Schaltfläche **Drucken** in der Symbolleiste.



Achtung! Der Text einer mit Formatierung erstellten Nachricht, die Bilder enthält, wird c Formatierung aber ohne Bilder ausgedruckt. Für nähere Informationen über die Einstellung der Druckparameter siehe den Abschnitt Druckparameter einstellen (auf S. 112).

Nachrichten und Anhänge im separaten Fenster anzeigen

So zeigen Sie die Nachricht in einem separaten Fenster an:

1. Doppelklicken Sie in der Nachrichtenliste auf die benötigte E–Mail oder wählen Sie die Nachricht in der Liste aus und drücken Sie anschließend die **Eingabetaste**. Es wird das Fenster zum Anzeigen einer Nachricht (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40) eingeblendet.

   Wenn es sich um eine ausgehende Nachricht handelt, die noch nicht gesendet oder digital signiert wurde, kann die Nachricht editiert werden (s. Verfassen der Nachricht auf S. 42).



Hinweis. Zum Editieren einer ungesendeten, digital signierten Nachricht entfernen Sie zunächst die digitale Signatur (s. Digitale Signatur löschen auf S. 72).

---

2. Zum Suchen innerhalb der Nachrichtentexte führen Sie folgende Schritte aus:
   - Wählen Sie im Menü **Bearbeiten** den Befehl **Suchen** oder drücken Sie die Tastenkombination **Strg+F**.
   - Geben Sie im Fenster **Suchen** die zu suchende Zeichenfolge ein.
   - Geben Sie, wenn nötig, zusätzliche Parameter und die Suchrichtung an.
   - Klicken Sie auf **Weitersuchen** oder drücken Sie **Enter**.
3. Die Liste der Empfänger wird in der Registerkarte Empfänger angezeigt (wird standardmäßig geöffnet).
   - Wenn links vom Empfängernamen das Symbol aufscheint, dann wurde von diesem Empfänger für den aktuellen Benutzer eine Notiz verfasst.
   - Klicken Sie mit der rechten Maustaste auf den Empfänger und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**, um Empfängerdetails anzuzeigen.
4. Öffnen Sie die Registerkarte **Anhänge**, um Anlagen anzuzeigen. Für Anhänge sind die folgenden Aktionen möglich:
   - Doppelklicken Sie auf den Anhang oder markieren Sie ihn und drücken Sie anschließend die **Eingabetaste**, um die angehängte Datei zu öffnen. Im Dialogfeld zur Bestätigung der Anzeige klicken Sie auf **OK**. Der Anhang wird in einem separaten Fenster geöffnet.
   - Wenn die Nachricht noch nicht versendet und der Anhang nicht digital signiert ist, kann der Anhang modifiziert werden. Klicken Sie mit der rechten Maustaste auf den Anhang und wählen Sie im Kontextmenü **Ansicht**. Der Anhang wird mit seinem Standardprogramm geöffnet.



Hinweis. Die am geöffneten Anhang vorgenommenen Änderungen können nicht gespeichert werden.

- Klicken Sie mit der rechten Maustaste auf den Anhang und wählen Sie im Kontextmenü **Datei kopieren**, um die angehängte Datei zu kopieren und in einer andere „Business Mail" Nachricht einzufügen.

  Klicken Sie mit der rechten Maustaste innerhalb der Registerkarte **Anhänge** und wählen Sie im Kontextmenü **Einfügen**, um den kopierten Anhang einzufügen.
- Klicken Sie mit der rechten Maustaste auf den Anhang und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**, um die Eigenschaften der Anlage anzuzeigen.
- Führen Sie einen der folgenden Schritte aus, um den Anhang zu speichern:
  - Klicken Sie mit der rechten Maustaste auf den Anhang und wählen im Kontextmenü **Speichern**. Im Fenster **Speichern unter** geben Sie den Ordner und den Dateinamen für die Speicherung an.
  - Klicken Sie mit der rechten Maustaste innerhalb der Registerkarte **Anhänge** und wählen im Kontextmenü **Speichern alles**, um alle Anhänge einer Nachricht zu speichern. Im Fenster **Durchsuchen** geben Sie den Ordner für die Speicherung an.
  - Klicken Sie auf einen Anhang und ziehen Sie ihn in den Ordner, in dem er gespeichert werden soll.
- Klicken Sie mit der rechten Maustaste auf den Anhang und wählen im Kontextmenü **Drucken**, um den Anhang auszudrucken.

5 Klicken Sie in der Symbolleiste auf die Schaltfläche **Drucken**, um den Nachrichtentext auszudrucken.



Achtung! Der Text einer mit Formatierung erstellten Nachricht, die Bilder enthält, wird c Formatierung aber ohne Bilder ausgedruckt. Für nähere Informationen über die Einstellung der Druckparameter siehe den Abschnitt Druckparameter einstellen (auf S. 112).

Nachricht beantworten und weiterleiten

Führen Sie folgende Schritte aus, um eine Nachricht zu beantworten oder weiterzuleiten:

1 Wählen Sie in der Navigationsleiste des ViPNet Business Mail Hauptfensters (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31)den Ordner, in dem sich die benötigte Nachricht befindet.

2 Wählen Sie die Nachricht in der Liste aus oder öffnen Sie sie in einem separaten Fenster (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40).

3 Führen Sie eine der folgenden Aktionen aus, um die Nachricht zu beantworten:

   - Klicken Sie mit der rechten Maustaste auf die Nachricht in der Liste und wählen Sie im Kontextmenü den Eintrag **Antworten** oder **Antworten mit Anhängen** (dieser Eintrag ist nur dann verfügbar, wenn die Nachricht Anhänge enthält).
   - Klicken Sie in der Symbolleiste des „Business Mail“ Hauptfensters oder des offenen Nachrichtenfensters auf die Schaltfläche **Antworten** , und wählen Sie im Untermenü den Eintrag **Antworten** oder **Antworten mit Anhängen** (dieser Eintrag ist nur dann verfügbar, wenn die Nachricht Anhänge enthält).

   Es wird das Fenster zum Verfassen einer Nachricht geöffnet. In der Betreffzeile der neuen Nachricht wird der Betreff der Originalnachricht mit dem Präfix „Re:“ angezeigt. Als Empfänger wird der Absender der Originalnachricht angegeben. Im Nachrichtentext werden die wichtigsten Details sowie der Text der Originalnachricht aufgeführt. Falls eine Antwort mit Anhängen gewählt wurde, werden der neuen Nachricht die Anlagen der Originalnachricht hinzugefügt.

4 Führen Sie die folgenden Schritte aus, um dem Absender oder allen Empfängern der Originalnachricht zu antworten:

   - Klicken Sie mit der rechten Maustaste auf die Nachricht in der Liste und wählen Sie im Kontextmenü den Eintrag **Allen antworten** oder **Allen antworten mit Anhängen** (dieser Eintrag ist nur dann verfügbar, wenn die Nachricht Anhänge enthält).
   - Klicken Sie in der Symbolleiste des „Business Mail“ Hauptfensters oder des offenen Nachrichtenfensters auf die Schaltfläche **Allen Antworten** oder **Allen antworten mit Anhängen** (dieser Eintrag ist nur dann verfügbar, wenn die Nachricht Anhänge enthält).

     Es wird das Fenster zum Verfassen einer Nachricht geöffnet. In der Betreffzeile der neuen Nachricht wird der Betreff der Originalnachricht mit dem Präfix „Re:“ angezeigt. Als Empfänger werden der Absender und alle Empfänger der Originalnachricht angegeben (mit Ausnahme der Benutzer des aktuellen Netzwerkknotens). Im Nachrichtentext werden die wichtigsten Details sowie der Text der Originalnachricht aufgeführt. Falls eine Antwort mit Anhängen gewählt wurde, werden der neuen Nachricht die Anlagen der Originalnachricht hinzugefügt.



Hinweis. Nach dem Beantworten einer Nachricht gilt der Text dieser Nachricht als gelesen.

5 Führen Sie einen der folgenden Schritte aus, um eine Nachricht weiterzuleiten:

- Klicken Sie mit der rechten Maustaste auf die Nachricht in der Liste und wählen Sie im Kontextmenü den Befehl **Weiterleiten**.
- Klicken Sie in der Symbolleiste des „Business Mail“ Hauptfensters oder des offenen Nachrichtenfensters auf die Schaltfläche **Weiterleiten** .

  Es wird das Fenster zum Verfassen einer Nachricht geöffnet. In der Betreffzeile der neuen Nachricht wird der Betreff der Originalnachricht mit dem Präfix „Fw:“ angezeigt. Im Nachrichtentext werden die wichtigsten Details sowie der Text der Originalnachricht angegeben. Falls die Originalnachricht Anhänge enthält, werden diese an die neue Nachricht angehängt.

6 Schließen Sie das Verfassen der Nachricht ab und versenden die E–Mail anschließend wie im Abschnitt Verfassen der Nachricht (auf S. 42).

Nachrichten suchen

Führen Sie folgende Schritte aus, um Nachrichten in „Business Mail“ zu suchen:

1. Wählen Sie im ViPNet Business Mail Hauptfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Nachrichten suchen**. Es wird das Fenster **Dokument suchen** eingeblendet.

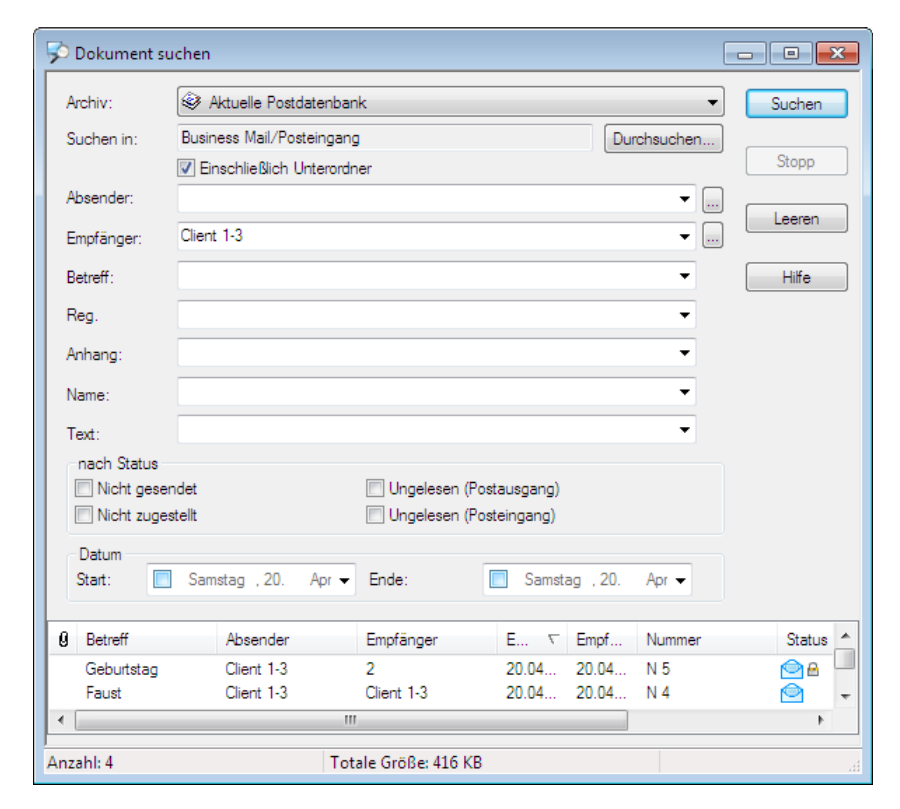


Abbildung 13. Fenster für die Nachrichtensuche

2. Wählen Sie in der Dropdownliste **Archiv** die Postdatenbank oder das Archiv aus, in dem gesucht werden soll.
3. Klicken Sie auf die Schaltfläche **Suchen** neben dem Feld **Suchen in** und wählen im Fenster **Ordner auswählen** den Ordner, in dem gesucht werden soll.
4. Aktivieren Sie das Kontrollkästchen **Einschließlich Unterordner**, um im gewählten Ordner inklusive aller Unterordner zu suchen.
5. Klicken Sie auf die Schaltfläche ... neben dem Feld **Absender** und wählen Sie im Adressbuch (s. Das Adressbuch auf S. 37) den betroffenen Absender aus, um den Absender der gesuchten Nachrichten anzugeben.
6. Klicken Sie auf die Schaltfläche ... neben dem Feld Absender und wählen Sie im Adressbuch (s. Das Adressbuch auf S. 37) den betroffenen Empfänger aus, um den Empfänger der gesuchten Nachrichten anzugeben.
7. Geben Sie im Feld **Betreff** einen Text an, um Nachrichten zu suchen, deren Betreffzeile diesen Text enthält.

8 Geben Sie im Feld **Reg.** die Nummer oder den permanenten Teil der Registrierungsnummer an, um Nachrichten nach der Registrierungsnummer zu suchen.

9 Geben Sie im Feld **Anhang** einen Teil des Anlagenamens an, um Nachrichten zu suchen, die Anhänge mit diesen Namen enthalten.

10 Geben Sie im Feld Name einen Teil des Dateinamens an, um Nachrichten nach dem Namen der Transportdatei (s. Datei (Transportdatei) auf S. 177) zu suchen.

11 Geben Sie im Feld **Text** eine Zeichenfolge ein, um Nachrichten zu suchen, deren Text diese Zeichenfolge enthält.

12 Aktivieren Sie in der Gruppe **nach Status** die benötigten Kontrollkästchen, um Nachrichten nach ihrem Sende-, Zustell- oder Lesestatus zu suchen.

- **Nicht gesendet**.
- **Nicht zugestellt**.
- **Ungelesen** (**Postausgang**).
- **Ungelesen** (**Posteingang**).

13 Führen Sie die folgenden Schritte aus, um Nachrichten in einem bestimmten Zeitabschnitt zu suchen:

- Aktivieren Sie das Kontrollkästchen im Feld **Start**, klicken Sie im rechten Teil des Feldes auf und wählen Sie mit Hilfe des Kalenderelements ein Datum, um den Beginn des Zeitabschnitts zu bestimmen.
- Aktivieren Sie das Kontrollkästchen im Feld **Ende**, klicken Sie im rechten Teil des Feldes auf und wählen Sie mit Hilfe des Kalenderelements ein Datum, um das Ende des Zeitabschnitts zu bestimmen.

14 Wenn Sie alle Suchparameter zurücksetzen wollen, klicken Sie auf die Schaltfläche **Löschen**.

15 Klicken Sie auf **Suchen**, um die Suche mit Hilfe der angegebenen Suchparameter zu starten.

Klicken Sie auf **Stopp**, um den Suchvorgang anzuhalten.

Alle Nachrichten, die den angegebenen Suchparametern entsprechen, werden in der Liste im unteren Bereich des Fensters Suchen angezeigt. Folgende Aktionen sind in der Ergebnisliste möglich:

- Mit Hilfe des Kontextmenüs können für die gefundenen Nachrichten die wichtigsten Aktionen ausgeführt werden: verschlüsseln, entschlüsseln, signieren, Signatur prüfen usw.
- Doppelklicken Sie auf eine gefundene Nachricht, um sie anzuzeigen.
- Wählen Sie im Kontextmenü den Punkt **Zum Hauptfenster wechseln**, um zum Ordner zu gelangen, der die gefundene Nachricht enthält.

Nachrichten exportieren und importieren

Nachrichten exportieren

Nachrichten können im BML-Format (das programminterne Format von ViPNet Business Mail) exportiert werden. Beim Export werden die digitale Signatur sowie der Zeitpunkt der letzten erfolgreichen Gültigkeitsprüfung der Signatur mit gespeichert. Falls die Nachrichten verschlüsselt sind, werden sie beim Export automatisch entschlüsselt.

Führen Sie die folgenden Schritte aus, um ViPNet Business Mail Nachrichten in einer `*.bml` Datei zu speichern:

1. Wählen Sie in der Navigationsleiste des ViPNet Business Mail Hauptfensters (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) den Ordner, in dem sich die zu exportierenden Nachrichten befinden.
2. Wählen Sie eine oder mehrere Nachrichten in der Liste aus.
3. Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen Sie im Kontextmenü einen der folgenden Punkte:
    - **Speichern unter**. Nach Auswahl dieses Befehls geben Sie im Fenster **Speichern** unter für jede Nachricht den Ordner und den Dateinamen für die Speicherung an und klicken dann auf **OK**.
    - **Speichern**. Nach Auswahl dieses Befehls geben Sie im Dialogfenster **Durchsuchen** den Ordner an, in dem die gewählten Nachrichten gespeichert werden sollen, und klicken auf **OK**. Der Name wird für jede Datei automatisch aus dem Text des Betreffs und der Registrierungsnummer zusammengestellt.

    Die Nachrichten werden als `*.bml` Dateien in den angegebenen Ordnern gespeichert.

Führen Sie einen der folgenden Schritte aus, um eine „Business Mail" Nachricht nach Microsoft Outlook oder Outlook Express (Windows Mail) zu exportieren:

- Ziehen Sie die Nachricht aus dem „Business Mail" Hauptfenster in das offene Fenster zum Erstellen einer neuen Nachricht in Microsoft Outlook oder Outlook Express. Die übertragene Nachricht wird in der neuen E–Mail als Anhang eingefügt.
- Ziehen Sie die Nachricht aus dem „Business Mail" Hauptfenster in irgendeinen Ordner im Hauptfenster von Microsoft Outlook oder Outlook Express. Im gewählten Ordner erscheint eine Nachricht, in die die übertragene „Business Mail" Nachricht eingefügt ist.



Hinweis. Wenn im gewählten Ordner das Erstellen neuer E–Mails nicht möglich ist, wird ein neues Nachrichtenfenster geöffnet, in dem die übertragene „Business Mail" Nachricht als Anhang eingefügt ist.

- Fügen Sie in einer Microsoft Outlook oder Outlook Express Nachricht die im Format `*.bml` exportierte „Business Mail“ Nachricht ein.

Nachrichten importieren

Nachrichten, die im BML-Format (das programminterne Format von ViPNet Business Mail) gespeichert sind, können importiert werden. Führen Sie einen der folgenden Schritte aus, um eine Nachricht zu importieren:

- Wählen Sie im Programmfenster im Menü **Extras** den Eintrag **Nachrichten importieren**. Geben Sie im Fenster **Öffnen** eine oder mehrere Dateien für den Import an und klicken Sie auf **Öffnen**.
- Ziehen Sie die zu importierenden Dateien mit der Maus in den Ordner **Import** im Hauptfenster von Vipnet Business Mail.

  Die importierten Nachrichten werden im Ordner **Import** abgelegt.

So übertragen Sie Microsoft Outlook oder Outlook Express (Windows Mail) Nachrichten nach VipNet Business Mail:

1. Führen Sie einen der folgenden Schritte aus:
   - Ziehen Sie eine oder mehrere E–Mails aus dem Microsoft Outlook oder Outlook Express Hauptfenster in einen Ordner in der Ordnerleiste von ViPNet Business Mail (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31).

     Es wird das Fenster zum Verfassen einer neuen Nachricht geöffnet. Gleichzeitig wird für jede übertragene Nachricht das Fenster **Namen des Anhangs eingeben** geöffnet.
   - Klicken Sie auf **Alle hinzufügen**, um alle Nachrichten als Dateien unter Beibehaltung ihrer Namen anzuhängen. Um die Dateinamen zu ändern, geben Sie für jeden Anhang einen Namen ein und klicken Sie auf **Hinzufügen**.

   Die E–Mails werden in der neuen Nachricht als Anhänge hinzugefügt.
2. Schließen Sie das Verfassen der Nachricht ab (s. Verfassen der Nachricht auf S. 42).

Nachrichten in andere Programmsordner verschieben

In „Business Mail“ können Nachrichten auf zwei Arten in andere Ordner verschoben werden:

- Wählen Sie in der Nachrichtenliste eine oder mehrere Nachrichten aus und verschieben Sie sie in den Zielordner.
- Führen Sie die folgenden Schritte aus:
    - Wählen Sie eine oder mehrere Nachrichten.
    - Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen Sie im Kontextmenü den Eintrag **Verschieben**.
    - Geben Sie im Fenster **Ordner auswählen** den Ordner an, in den die Nachrichten verschoben werden sollen, und klicken auf **OK**.

Beim Verschieben von Nachrichten gelten folgende Einschränkungen:

- Nachrichten können nicht aus dem Ordner **Posteingang** und **Gelöschte Objekte** > **Posteingang** in die Ordner **Postausgang** und **Gelöschte Objekte** > **Postausgang** verschoben werden.
- Nachrichten können nicht aus dem Ordner **Postausgang** in den Ordner **Gelöschte Objekte** > **Posteingang** verschoben werden.
- In den Ordner **Posteingang** können Nachrichten nur aus dem Ordner **Gelöschte Objekte** > **Posteingang** verschoben werden und umgekehrt.
- Es können keine Nachrichten aus oder in den Ordner **Audit** verschoben werden.
- Es können keine Nachrichten zwischen zwei Unterordnern von **Gelöschte Objekte** oder **Audit** verschoben werden.

Nachrichten löschen

Führen Sie folgende Schritte aus, um Nachrichten aus beliebigen Ordnern mit Ausnahme von **Audit** und **Gelöschte Objekte** (einschließlich ihren Unterordnern) zu löschen:

1. Wählen Sie in der Nachrichtenliste eine oder mehrere Nachrichten aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Drücken Sie die **ENTF**–Taste.
   - Klicken Sie in der Symbolleiste auf **Löschen** .
   - Ziehen Sie die Nachricht in den Ordner **Gelöschte Objekte**.

   Die gewählten Nachrichten werden in den Ordner **Gelöschte Objekte** verschoben. Dabei wird im Ordner **Gelöschte Objekte** automatisch eine Ordnerstruktur erzeugt, die derjenigen entspricht, in der sich die Nachricht befunden hat. Zum Beispiel wird beim Löschen einer Nachricht aus **Posteingang** > **Ordner** die betroffene Nachricht in den Ordner **Gelöschte Objekte** > **Posteingang** > **Ordner** verschoben.



Hinweis. Beim Verschieben der Nachrichten in irgendeinen Unterordner von Gelöschte Objekte werden sie genau in diesen Unterordner verschoben. Zusätzliche Ordner werden dabei nicht erstellt. In manche Ordner können keine Nachrichten verschoben werden (s. Nachrichten in andere Programmsordner verschieben auf S. 58).

So entfernen Sie Nachrichten aus **Gelöschte Objekte**:

1. Wählen Sie eine oder mehrere Nachrichten aus.
2. Drücken Sie die **ENTF**–Taste oder klicken Sie auf **Löschen** .

   Im Ordner **Audit** wird eine genaue Kopie der Ordnerstruktur aus **Gelöschte Objekte** erzeugt, die einen Eintrag mit der Löschzeit und dem Namen des Benutzers enthält, der den Löschvorgang ausgelöst hat. Dieser Eintrag im Ordner **Audit** kann nur vom Netzwerkknoten-Administrator (s. Arbeiten mit Administratorrechten auf S. 114) entfernt werden.



Hinweis. Beim Arbeiten im Administrator–Modus ist im Kontextmenü der Befehl **Unwiderruflich löschen** (s. Zusätzliche Möglichkeiten und Parameter des Programms auf S. 114) verfügbar.

Nachrichten archivieren

Unter Archivierung versteht man das Verschieben von bestimmten Nachrichtenkategorien aus der aktuellen Postdatenbank von „Business Mail“ in einen bestimmten Ordner auf der Festplatte. Archivierung hilft, das Speichervolumen zu verkleinern und die Arbeit mit Nachrichten zu beschleunigen.

Bei der Archivierung werden die Nachrichten in einem Archivordner abgelegt, dessen Name das Datum und die Uhrzeit des Zeitpunkts der Archivierung beinhaltet, zum Beispiel 21092010_163539. Standardmäßig wird das Archiv im Ordner `\ViPNet Client\MSArch` erzeugt. Der Ordner für die Speicherung der Archive kann geändert werden (s. Arbeiten mit Nachrichtenarchiven auf S. 62).

Neben den Nachrichten werden auch Anhänge in das Archiv verschoben, wobei es beim Speichern der Anhänge im Archiv zwei Möglichkeiten gibt:

- Übertragung der Anhänge aus den Dateien in die Datenbank, um die Anhänge gemeinsam mit den Nachrichten im Archiv zu speichern.

  Bei dieser Art der Speicherung enthält das Archiv nur eine Datei. Dies erleichtert das Kopieren und Übertragen des Archivs auf einen externen Datenträger, um z. B. eine Backup-Kopie zu erstellen.

- Speicherung der Anhänge in gesonderten Ordnern.

  Bei dieser Art der Speicherung enthält das Archiv eine Datei mit der Nachrichtendatenbank und mehrere Ordner, in denen die Anhangdateien untergebracht sind.

Archivierte Nachrichten werden aus dem Nachrichtenspeicher von „Business Mail“-Programm entfernt und erscheinen nicht mehr im Programm, können aber eingesehen werden, falls das entsprechende Archiv geöffnet wird (s. Arbeiten mit Nachrichtenarchiven auf S. 62).

Eine Archivierung kann sowohl manuell gestartet werden als auch automatisch erfolgen. Die automatische Archivierung wird bei Erfüllung bestimmter Bedingungen gestartet. Kategorien von Nachrichten, die archiviert werden sollen, und weitere Parameter der automatischen Archivierung können im Fenster **Einstellungen** im Bereich **Archivierung** (s. Allgemeine Archivierungsparameter auf S. 105) eingestellt werden.

Führen Sie die folgenden Schritte aus, um Nachrichten zu archivieren:

1. Abhängig vom Archivierungsmodus:
   - Wählen Sie im Menü **Datei** des ViPNet Business Mail Hauptfensters den Eintrag **Nachrichten archivieren**, um die manuelle Archivierung zu starten.
   - Die automatische Archivierung wird in Abhängigkeit von den gesetzten Parametern (s. Allgemeine Archivierungsparameter auf S. 105) automatisch gestartet.
2. Vor Beginn der Archivierung wird ein Fenster zur Bestätigung des Archivierungsvorgangs eingeblendet. Wenn die Archivparameter (s. Allgemeine Archivierungsparameter auf S. 105) so konfiguriert wurden, dass nicht alle Nachrichten, sondern nur einige Kategorien von Nachrichten archiviert werden, dann wird eine Warnmeldung angezeigt, dass die Archivierung eine längere Zeit in Anspruch nehmen kann.

   Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um die Archivierung zu starten.

3. Wenn zum Zeitpunkt der Archivierung irgendwelche Nachrichten geöffnet sind, gibt das Programm die Meldung aus, dass alle Nachrichten zu schließen sind.

   Um die Archivierung abzubrechen, klicken Sie im Dialogfeld der Meldung auf die Schaltfläche **Nein**. Klicken Sie auf **Ja**, falls Sie fortfahren möchten; dabei werden alle offenen Nachrichten automatisch geschlossen.
4. Der Archivierungsprozess wird gestartet und kann über die Statusanzeige mitverfolgt werden.

   Alle zu archivierenden Nachrichten werden aus der Postdatenbank in das Archiv übertragen.

Arbeiten mit Nachrichtenarchiven

Das Programm „Business Mail“ erlaubt es, Archive der eigenen Nachrichten sowie Archive anderer Benutzer (soweit sie nicht verschlüsselt sind) einzusehen, sowie Archive zu verschieben, zu löschen und umzubenennen.

Führen Sie die folgenden Schritte aus, um ein Nachrichtenarchiv in „Business Mail“ zu öffnen:

1 Wählen Sie im Menü **Datei** des ViPNet Business Mail Hauptfensters den Eintrag **Archiv auswählen**. Es wird das Fenster **Archiv** eingeblendet.

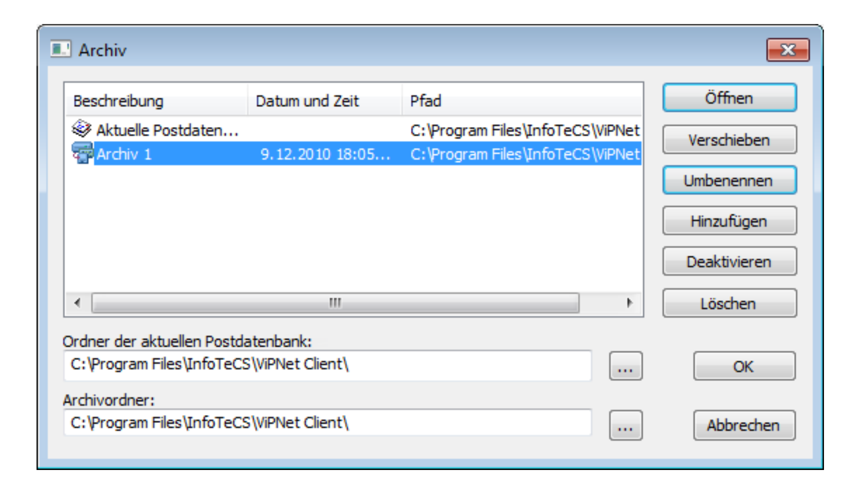


Abbildung 14. Fenster der Archivverwaltung

2 Wählen Sie in der Liste das Archiv aus, das Sie anzeigen möchten.

3 Klicken Sie auf **Öffnen**.

Nachrichten, die im gewählten Archiv enthalten sind, werden im „Business Mail“ Programmfenster angezeigt. Auf diese Nachrichten kann nur lesend zugegriffen werden. Gegebenenfalls können die Nachrichten aber mit Hilfe des Befehls **Verschlüsseln** (**Entschlüsseln**) im Kontextmenü verschlüsselt (entschlüsselt) werden.



Hinweis. Eine Nachricht, die im Archiv enthalten ist, kann nur dann verschlüsselt werden, wenn auf das Archiv schreibend zugegriffen werden kann.

Während der Arbeit mit einem Archiv ist die Postdatenbank von „Business Mail“ nicht verfügbar, das heißt, es können keine Nachrichten gesendet oder empfangen werden.

So kehren Sie zur aktuellen Postdatenbank zurück:

1 Wählen Sie im Menü **Datei** den Punkt **Archiv auswählen**. Es wird das Fenster **Archiv** eingeblendet.

2 Wählen Sie im Fenster **Archiv** in der Liste den Eintrag **Aktuelle Postdatenbank** aus.

3 Klicken Sie auf die Schaltfläche **Öffnen**.

Im „Business Mail“ Hauptfenster wird die aktuelle Postdatenbank geöffnet, in der Sie vollwertig mit geschützter Post arbeiten können.

Führen Sie die folgenden Schritte aus, um ein Nachrichtenarchiv anzuzeigen, das auf einem anderen Computer erstellt wurde (zum Beispiel das Archiv des Benutzers eines anderen Netzwerkknotens, das mittels Datenträger übergeben wurde):

1. Wählen Sie im Menü **Datei** den Eintrag **Archiv auswählen**. Es wird das Fenster **Archiv** eingeblendet.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**. Es wird das Fenster **Durchsuchen** eingeblendet.
3. Geben Sie im Fenster **Durchsuchen** den Ordner an, der das Nachrichtenarchiv enthält, und klicken auf **OK**.

   Das gewählte **Archiv** wird im Fenster Archiv in die Liste aufgenommen.
4. Wählen Sie dieses Archiv in der Liste aus und klicken auf **Öffnen**.

   Die im Archiv enthaltenen Nachrichten werden im Programmfenster von „Business Mail“ angezeigt. Auf diese Nachrichten kann nur lesend zugegriffen werden. Wenn im Archiv Nachrichten enthalten sind, die mit den Schlüsseln einer anderen Arbeitsgruppe verschlüsselt wurden, dann ist die Anzeige dieser Nachrichten nicht möglich.

Folgende Aktionen sind im Fenster **Archiv** außerdem möglich:

- So ändern Sie den Ordner der aktuellen Postdatenbank:
  - Klicken Sie auf die Schaltfläche [...] neben dem Eingabefeld **Ordner der aktuellen Postdatenbank**.
  - Geben Sie im Fenster **Durchsuchen** den Ordner an, in welchem sich die laufende Postdatenbank befinden soll, und klicken Sie auf **OK**.

  Beim nächsten Start des Programms ViPNet Business Mail wird im angegebenen Ordner die Unterordner `\MSArch` erstellt, wo die erstellten Nachrichtenarchive abgelegt werden.
- So verschieben Sie das Archiv in einen anderen Ordner:
  - Wählen Sie im Fenster Archiv ein **Archiv** aus und klicken Sie auf **Verschieben**.
  - Wählen Sie im Fenster **Durchsuchen** einen Ordner, in den das Archiv verschoben werden soll, und klicken auf **OK**. Das Archiv wird in den angegebenen Ordner verschoben.
- So benennen Sie ein Archiv um:
  - Wählen Sie im Fenster **Archiv** ein Archiv aus und klicken auf **Umbenennen**. Anstelle des Archivnamens erscheint in der Liste ein Eingabefeld.
  - Geben Sie den neuen Namen ein und drücken die **Eingabetaste**.
- Um ein Archiv aus der Liste zu entfernen, wählen Sie im Fenster Archiv ein Archiv aus und klicken auf die Schaltfläche **Deaktivieren**. Das Archiv wird aus der Liste entfernt, bleibt aber auf der Festplatte gespeichert.
- So löschen Sie ein Archiv:
  - Wählen Sie im Fenster **Archiv** ein Archiv aus, das gelöscht werden soll.

- Klicken Sie auf die Schaltfläche **Löschen**. Im Dialogfeld zur Bestätigung des Löschvorgangs klicken Sie auf **OK**.



Digitale Signatur und Verschlüsselung

Digitale Signatur in „Business Mail“

Die digitale Signatur ist ein Element des elektronischen Dokuments, das mit Hilfe eines kryptografischen Rechenverfahrens unter Verwendung eines privaten Signaturschlüssels aus der Nachrichteninformation gewonnen wird.

Die digitale Signatur erlaubt es:

- Die Authentizität des Dokuments zu bestätigen: die digitale Signatur identifiziert den Unterzeichner des Dokuments.
- Die Integrität des Dokuments zu bestätigen: die digitale Signatur bestätigt, dass das Dokument nach der Unterzeichnung nicht modifiziert wurde.
- Die Nichtabstreitbarkeit zu sichern: die digitale Signatur macht einen Verzicht des Unterzeichners auf die Urheberschaft des Dokuments unmöglich.

Mit Hilfe von „Business Mail“ können sowohl Nachrichten und ihre Anhänge (s. Arbeiten mit digitalen Signaturen von Nachrichten auf S. 67) als auch separate Dateien (s. Arbeiten mit digitalen Signaturen von Dateien auf S. 74) digital signiert werden. Außerdem können vorhandene digitale Signaturen von Nachrichten und Dateien geprüft oder entfernt werden.

Folgende Zertifikatstypen (s. Zertifikat auf S. 180) können für das Signieren von Nachrichten und Dateien verwendet werden:

- Signaturzertifikat des aktuellen Client–Benutzers.
- Signaturzertifikat des Benutzers eines anderen Netzwerkknotens oder Signaturzertifikat eines externen Benutzers des ViPNet Netzwerks (s. Signaturzertifikat auswählen auf S. 68), das sich in einem Container mit privatem Schlüssel befindet. Der Container kann auf der Festplatte oder auf einem externen Datenträger gespeichert sein (s. Externe Datenträger auf S. 174).
- Signaturzertifikat, das von einer externen Zertifizierungsstelle ausgestellt wurde (s. Verwendung von Signaturschlüsseln, die mit Hilfe des Cryptoproviders eines Drittherstellers erzeugt sind auf S. 70).

Arbeiten mit digitalen Signaturen von Nachrichten

Nachricht digital signieren

Das automatische Signieren von Nachrichten und Anhängen mit dem aktuellen Zertifikat ist in „Business Mail“ beim Absenden standardmäßig voreingestellt. Diese Einstellungen können im Bereich **Nachricht** (s. Nachrichtenparameter einstellen auf S. 109) geändert werden.

Führen Sie die folgenden Schritte aus, um eine oder mehrere Nachrichten digital zu signieren:

1 Wählen Sie im Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Ordner **Postausgang** (oder einem Unterordner davon) eine oder mehrere ungesendete Nachrichten, die digital signiert werden sollen.

2 Führen Sie einen der folgenden Schritte aus:

  - Klicken Sie in der Symbolleiste auf die Schaltfläche **Signieren** und wählen im Untermenü einen der Einträge aus:

    - **Aktuelles Zertifikat verwenden**, um die Nachrichten mit dem Signaturzertifikat des aktuellen Benutzers zu signieren.

    - **Anderes Zertifikat verwenden**, um Nachrichten mit einem Zertifikat aus einem bestimmten Container des privaten Schlüssels zu signieren.

  - Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen im Kontextmenü den Eintrag **Signieren**. Klicken Sie dann auf **Aktuelles Zertifikat verwenden** oder **Anderes Zertifikat verwenden**.

3 Wenn das Signieren mit Signaturzertifikat aus einem Schlüsselcontainer gewählt wurde, führen Sie die Schritte aus, die im Abschnitt Signaturzertifikat auswählen (auf S. 68) beschrieben sind.

  Die Nachrichten werden mit einer digitalen Signatur unterzeichnet und erhalten ein entsprechendes Statusattribut. Wenn die Nachrichten Anhänge enthalten, werden diese ebenfalls signiert.

Führen Sie die folgenden Schritte aus, um eine Nachricht zu signieren, die im Fenster zum Anzeigen und Verfassen von Nachrichten (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40) geöffnet ist:

1 Erstellen Sie eine neue Nachricht (s. Verfassen der Nachricht auf S. 42) oder öffnen eine ungesendete Nachricht in einem separaten Fenster.

2 Führen Sie einen der folgenden Schritte aus:

  - Klicken Sie in der Symbolleiste auf die Schaltfläche **Signieren** und wählen im Untermenü einen der Einträge aus:

- **Aktuelles Zertifikat verwenden**, um die Nachrichten mit dem Signaturzertifikat des aktuellen Benutzers zu signieren.
- **Anderes Zertifikat verwenden**, um Nachrichten mit einem Zertifikat aus einem bestimmten Container des privaten Schlüssels zu signieren.

  - Klicken Sie im Menü **Signieren** auf den Eintrag **Ganze Nachricht digital signieren** und wählen im Untermenü **Aktuelles Zertifikat verwenden** oder **Anderes Zertifikat verwenden**.

3. Wenn das Signieren mit Signaturzertifikat aus einem Schlüsselcontainer gewählt wurde, führen Sie die Schritte aus, die im Abschnitt Signaturzertifikat auswählen (auf S. 68) beschrieben sind.

   Die Nachricht und ihre Anhänge werden digital signiert.

Führen Sie die folgenden Schritte aus, um nur den Nachrichtentext digital zu signieren:

1. Erstellen Sie eine neue Nachricht oder öffnen eine ungesendete Nachricht in einem separaten Fenster.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie im Menü **Signieren** auf den Eintrag **Nachrichtentext digital signieren** und wählen im Untermenü **Aktuelles Zertifikat verwenden** oder **Anderes Zertifikat verwenden**.
   - Klicken Sie mit der rechten Maustaste auf den Nachrichtentext und wählen im Kontextmenü den Eintrag **Nachrichtentext digital signieren**. Klicken Sie dann auf **Aktuelles Zertifikat verwenden** oder **Anderes Zertifikat verwenden**.
3. Wenn das Signieren mit Signaturzertifikat aus einem Schlüsselcontainer gewählt wurde, führen Sie die Schritte aus, die im Abschnitt Signaturzertifikat auswählen (auf S. 68) beschrieben sind.

   Der Nachrichtentext wird digital signiert.

So signieren Sie nur die Anhänge einer Nachricht:

1. Erstellen Sie eine neue Nachricht oder öffnen eine ungesendete Nachricht in einem separaten Fenster.
2. Fügen Sie der Nachricht einen oder mehrere Anhänge hinzu.
3. Wählen Sie in der Registerkarte **Anhänge** einen oder mehrere Anhänge.
4. Klicken Sie mit der rechten Maustaste auf die gewählten Anhänge und wählen im Kontextmenü den Eintrag **Signieren**. Klicken Sie dann auf **Aktuelles Zertifikat verwenden** oder **Anderes Zertifikat verwenden**.
5. Wenn das Signieren mit Signaturzertifikat aus einem Schlüsselcontainer gewählt wurde, führen Sie die Schritte aus, die im Abschnitt Signaturzertifikat auswählen (auf S. 68) beschrieben sind.

   Die gewählten Anhänge werden digital signiert.

Signaturzertifikat auswählen

Wenn beim Signieren der Datei oder Nachricht mit einer digitalen Signatur der Befehl **Anderes Zertifikat verwenden** gewählt wurde, dann wird das Fenster **Initialisierung des Schlüssel–Containers** geöffnet.

Wenn sich der Container auf der Festplatte befindet, dann führen Sie folgende Schritte aus, um ein Zertifikat auszuwählen:

1 Wählen Sie im Fenster **Initialisierung des Schlüssel–Containers** die Option **Ordner**.

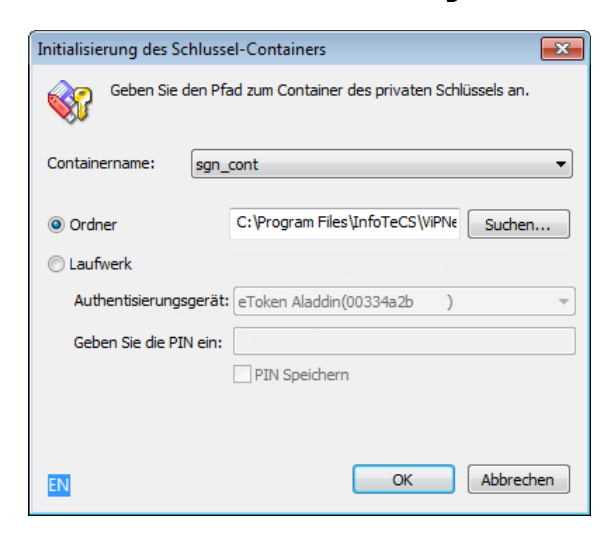


Abbildung 15. Schlüsselcontainer auf der Festplatte

2 Klicken Sie auf die Schaltfläche **Suchen** und wählen den Pfad des Ordners, in dem sich der Container befindet.

3 Wenn sich mehrere Container im Ordner befinden, wählen Sie in der Liste **Containername** den benötigten Container aus.

4 Klicken Sie auf **OK**.

5 Wenn sich im Container mehrere Zertifikate befinden, wird das Fenster **Anderes Zertifikat verwenden** geöffnet. Wählen Sie ein Zertifikat aus und klicken auf **OK**.

6 Geben Sie im Fenster **ViPNet CSP – Passwort des Schlüsselcontainers** das Passwort für den Zugriff auf den Container ein und klicken auf **OK**.

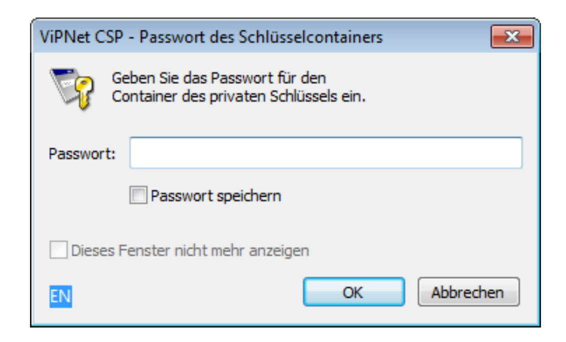


Abbildung 16. Passwort für den Container des privaten Schlüssels eingeben

Die Nachricht (oder Datei) wird mit dem gewählten Signaturzertifikat signiert.

Wenn sich der Container auf externen Datenträger (s. Liste externer Datenträger auf S. 175) befindet, führen Sie die folgenden Schritte aus:

1 Wählen Sie im Fenster **Initialisierung des Schlüssel–Containers** die Option **Authentisierungsgerät**.

2 Schließen Sie das Gerät an, auf dem der Container gespeichert ist. Wenn mehrere Authentisierungsgeräte angeschlossen sind, wählen Sie in der Liste **Gerät auswählen** das benötigte Gerät aus.

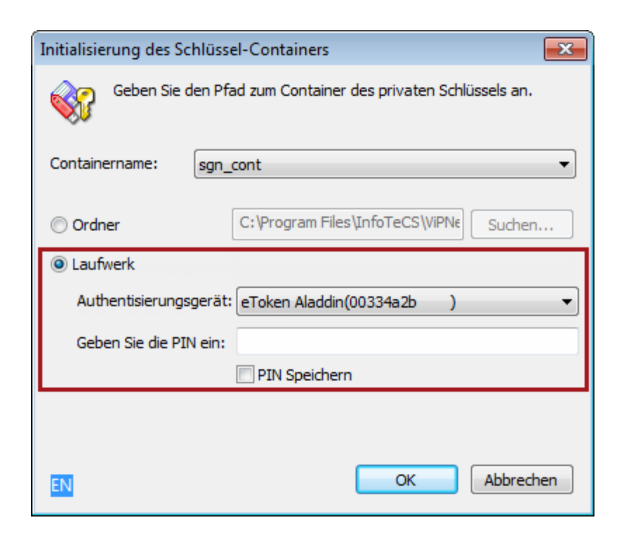


Abbildung 17. Schlüsselcontainer auf einem Authentisierungsgerät

3 Wenn sich mehrere Container auf dem Gerät befinden, wählen Sie in der Liste **Containername** den benötigten Container aus.

4 Geben Sie im Feld **Geben Sie die PIN ein** die benötigte PIN an.

Die Nachricht (oder Datei) wird mit dem gewählten Signaturzertifikat signiert.

Verwendung von Signaturschlüsseln, die mit Hilfe des Cryptoproviders eines Drittherstellers erzeugt sind

Nachrichten und Dateien können in „Business Mail" mit Zertifikaten signiert werden, die von externen Zertifizierungsstellen, die nicht Teil des geschützten ViPNet Netzwerks sind, ausgestellt wurden.

Führen Sie die folgenden Schritte aus, um ein solches Zertifikat zu verwenden:

1 Im Programm ViPNet CSP deaktivieren Sie den Cryptoprovider.

2 Installieren Sie einen Cryptoprovider, der für die Arbeit mit dem externen Zertifikat notwendig ist.

3 Installieren Sie das Zertifikat und den entsprechenden privaten Schlüssel in den persönlichen Zertifikatspeicher mit Hilfe des Programms „Zertifikate – aktueller Benutzer" (certmgr.msc).

Benutzen Sie die Windows–Hilfe, um weitere Informationen über den Import von Zertifikaten zu erhalten.

4 Stellen Sie sicher, dass ein privater dem installierten Zertifikat entsprechender Schlüssel vorhanden ist.



Hinweis. Der verwendete Cryptoprovider bestimmt, wie das Zertifikat erhalten und installiert wird sowie welcher private Schlüssel dem Zertifikat entspricht.

5 Stellen Sie sicher, dass im Fenster Sicherheitseinstellungen in der Registerkarte Administrator das Kontrollkästchen **Benutzung externer Zertifikate erlauben** (s. Zusätzliche Sicherheitseinstellungen auf S. 115) aktiviert ist.



Hinweis. Die Änderungen der Einstellungen in der Registerkarte Administrator können nur vom Netzwerkknoten-Administrator (s. Arbeiten mit Administratorrechten auf S. 114) vorgenommen werden

6 Wählen Sie in der Registerkarte **Signieren** das benötigte Zertifikat aus, das als aktuelles Zertifikat dienen soll (s. Laufendes Zertifikat wechseln auf S. 143).

7 Beim Signieren von Nachrichten (s. Nachricht digital signieren auf S. 67) und Dateien (s. Datei digital signieren auf S. 74) wählen Sie im Menü den punkt **Aktuelles Zertifikat verwenden**.

Digitale Signatur überprüfen

Führen Sie die folgenden Schritte aus, um die digitale Signatur einer Nachricht zu überprüfen:

1 Wählen Sie im ViPNet Business Mail Hauptfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) eine Nachricht aus der Liste aus (mit Symbol oder), für die die digitale Signatur überprüft werden soll.

2 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Prüfen** .
- Klicken Sie mit der rechten Maustaste auf die Nachricht und wählen im Kontextmenü den Eintrag **Signatur überprüfen**.

Es wird das Fenster **Ergebnis der Signaturüberprüfung** geöffnet.

Führen Sie die folgenden Schritte aus, um im Nachrichtenfenster (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40) die digitale Signatur einer Anlage zu überprüfen:

1 Öffnen Sie die Nachricht, die einen signierten Anhang enthält, in einem separaten Fenster.

2 Klicken Sie in der Registerkarte **Anhänge** mit der rechten Maustaste auf die betreffende Anlage und wählen im Kontextmenü den Punkt **Signatur überprüfen**.

Es wird das Fenster **Ergebnis der Signaturüberprüfung** geöffnet.

Das Fenster **Ergebnis der Signaturüberprüfung** enthält Informationen über digitale Signaturen jedes Bestandteils einer Nachricht (Text und Anhänge). Gültige Signaturen sind mit einem grünen Symbol gekennzeichnet, ungültige mit einem roten.

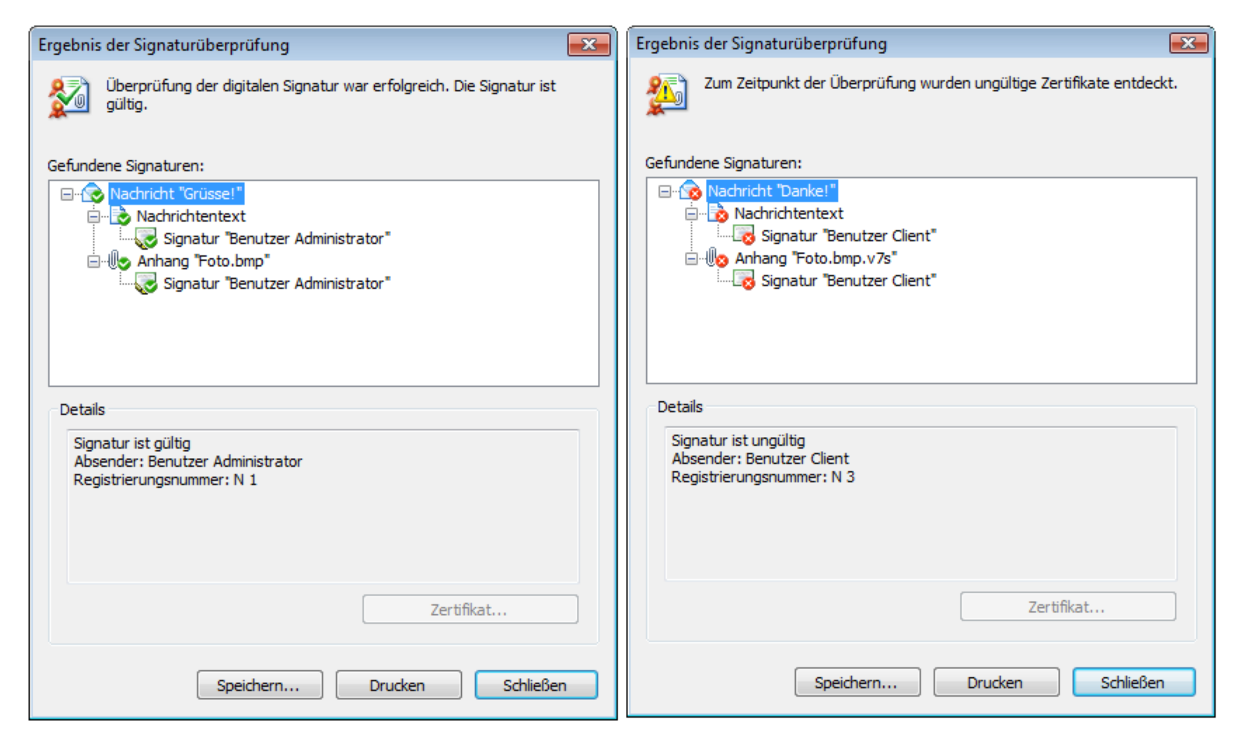


Abbildung 18. Ergebnis der Signaturüberprüfung

Im Fenster **Ergebnis der Signaturüberprüfung** sind folgende Aktionen möglich:

- Wählen Sie im Bereich **Gefundene Signaturen** ein Nachrichtenelement aus, um Informationen über die digitale Signatur dieses Elements (gesamte Nachricht, Text, irgendein Anhang oder digitale Signatur) zu erhalten. Die Information über die Signatur wird im Bereich **Details** eingeblendet.
- Wählen Sie im Bereich **Gefundene Signaturen** eine digitale Signatur aus und klicken auf die Schaltfläche Zertifikat, um das Zertifikat zu sehen, mit dem die Nachricht signiert wurde.

Digitale Signatur löschen

Führen Sie die folgenden Schritte aus, um die digitale Signatur einer oder mehrerer Nachrichten zu löschen:

1. Wählen Sie im ViPNet Business Mail Hauptfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Ordner **Postausgang** (oder einem Unterordner davon) eine oder mehrere ungesendete Nachrichten mit digitalen Signaturen aus (sie besitzen das Symbol oder).
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Entfernen** .
   - Klicken Sie mit der rechten Maustaste auf die Nachricht und wählen im Kontextmenü den Eintrag **Digitale Signatur entfernen**.

   Die digitalen Signaturen der gewählten Nachrichten und ihrer Anhänge werden entfernt.

So entfernen Sie die digitale Signatur einer im Fenster zum Anzeigen und Verfassen von Nachrichten (auf S. 40) geöffneten Nachricht:

- Klicken Sie in der Symbolleiste auf **Entfernen** , um die digitale Signatur des Nachrichtentextes und aller Anhänge zu entfernen.
- Klicken Sie in der Registerkarte Anhänge mit der rechten Maustaste auf einen signierten Anhang und wählen im Kontextmenü den Eintrag **Signatur entfernen**, um die digitale Signatur einer Anlage zu löschen.
- Klicken Sie mit der rechten Maustaste in den Bereich des Nachrichtentextes und wählen im Kontextmenü den Eintrag **Digitale Signatur aus dem Nachrichtentext entfernen**, um die digitale Signatur des Nachrichtentextes zu entfernen (wenn dieser signiert ist).

Arbeiten mit digitalen Signaturen von Dateien

Datei digital signieren

Das Programm „Business Mail“ erlaubt es, Dateien mit einer digitalen Signatur zu unterzeichnen, die nicht Anhänge einer „Business Mail“ Nachricht sind. Die signierte Datei erhält die Erweiterung `.v7s`. Zum Beispiel wird die Datei `Document.txt` nach dem Signieren durch die Datei `Document.txt.v7s` ersetzt.

Die signierte Datei mit der Erweiterung `.v7s` kann weder angezeigt noch modifiziert werden. Beim Versuch, die Datei zu öffnen, wird eine Überprüfung der digitalen Signatur gestartet (s. Dateisignatur überprüfen auf S. 75). Um die Möglichkeit zu haben, eine signierte Datei anzuzeigen, muss ihre digitale Signatur von der Datei getrennt werden (s. Dateisignatur anhängen und abtrennen auf S. 75). Falls die Datei mit einer existierenden oder abgetrennten Signatur modifiziert wird, so wird die digitale Signatur ungültig.

Führen Sie die folgenden Schritte aus, um eine oder mehrere Dateien digital zu signieren, die nicht Anhang einer „Business Mail“ Nachricht sind:

1. Klicken Sie im ViPNet Business Mail Hauptfenster im Menü **Datei** auf den Eintrag **Datei signieren**, dann wählen Sie:
   - **Mit aktuellem Zertifikat signieren**, um für die Signatur das laufende Signaturzertifikat zu verwenden.
   - **Die Datei mit anderem Zertifikat signieren**, um für die Signatur das Signaturzertifikat aus einem externen Container zu verwenden.
2. Wenn das Signieren mit einem externen Zertifikat gewählt wurde, führen Sie die im Abschnitt Signaturzertifikat auswählen (auf S. 68).
3. Es wird das Fenster **Öffnen** eingeblendet. Wählen Sie in diesem Fenster eine oder mehrere Dateien aus, die digital signiert werden sollen, und klicken auf **Öffnen**.
4. Wenn für die Signatur ein externes Zertifikat gewählt wurde, das sich in einem Container auf der Festplatte befindet, geben Sie im Fenster **ViPNet CSP - Passwort des Schlüsselcontainers** (s. Abbildung auf S. 161) das Passwort für den Zugriff auf den Container ein.

   Die Dateien werden mit dem gewählten Zertifikat signiert.



Hinweis. Ein und dieselbe Datei kann mit unterschiedlichen Signaturzertifikaten mehrmals signiert werden.

Wenn eine Datei signiert wird, die eine getrennte digitale Signatur besitzt (s. Dateisignatur anhängen und abtrennen auf S. 75), wird die neue Signatur an die Datei angehängt, und die abgetrennte Signatur bleibt unverändert.

Dateisignatur anhängen und abtrennen

Beim Signieren der Datei mit einer oder mehreren digitalen Signaturen wird eine `*.v7s` Datei erzeugt, die die Originaldatei mitsamt den digitalen Signaturen beinhaltet.

Führen Sie folgende Schritte aus, um die Signatur von der Datei zu trennen:

1. Klicken Sie im ViPNet Business Mail Hauptfenster im Menü **Datei** auf den Eintrag **Datei signieren**, dann wählen Sie **Signatur abtrennen**.
2. Geben Sie im Fenster **Öffnen** eine oder mehrere Dateien mit der Erweiterung `.v7s` an, die von ihren digitalen Signaturen getrennt werden sollen, und klicken auf **Öffnen**.

   Die digitalen Signaturen werden von den Dateien getrennt. Die Dateien nehmen den ursprünglichen Zustand an, die abgetrennten Signaturen werden in Dateien mit der Erweiterung `.p7s` gespeichert.

   Wenn zum Beispiel die digitale Signatur von der Datei `Document.txt.v7s` abgetrennt wird, bleiben als Ergebnis zwei Dateien über: `Document.txt` und `Document.txt.p7s`.



Hinweis. Wenn eine Datei gleichzeitig eine abgetrennte und eine angehängte digitale Signatur besitzt, wird die angehängte Signatur in der Datei `*.p7s` abgelegt, indem die vorhandene Datei mit der abgetrennten Signatur ersetzt wird.

Führen Sie die folgenden Schritte aus, um eine abgetrennte digitale Signatur wieder anzuhängen:

1. Klicken Sie im ViPNet Business Mail Hauptfenster im Menü **Datei** auf den Eintrag **Datei signieren**, dann wählen Sie **Signatur abhängen**.
2. Geben Sie im Fenster **Öffnen** eine oder mehrere Dateien an, die abgetrennte Signaturen besitzen, und klicken auf die Schaltfläche **Öffnen**. Wenn zum Beispiel die Datei `Document.txt` eine abgetrennte Signatur `Document.txt.p7s` besitzt, so wählen Sie zum Hinzufügen der Signatur die Datei `Document.txt`.

   An die gewählten Dateien werden digitale Signaturen angehängt. Die Dateien werden dementsprechend durch `*.v7s` Dateien ersetzt.



Hinweis. Wenn die Datei gleichzeitig eine angehängte und eine abgetrennte digitale Signatur besitzt, so ist das Anhängen der abgetrennten Signatur nur nach dem Entfernen der vorhandenen Signatur möglich.

Dateisignatur überprüfen

Führen Sie die folgenden Schritte aus, um die digitale Signatur einer Datei zu überprüfen:

1. Klicken Sie im ViPNet Business Mail Hauptfenster im Menü **Datei** auf den Eintrag **Datei signieren**, dann wählen Sie **Unterschrift überprüfen**.

2 Geben Sie im Fenster **Öffnen** eine oder mehrere Dateien an, die angehängte oder getrennte digitale Signaturen besitzen (zum Beispiel `Document.txt.v7s` oder `Document.txt`, aber nicht `Document.txt.p7s`).

3 Klicken Sie auf Öffnen. Es wird das Fenster **Ergebnis der Signaturüberprüfung** eingeblendet.

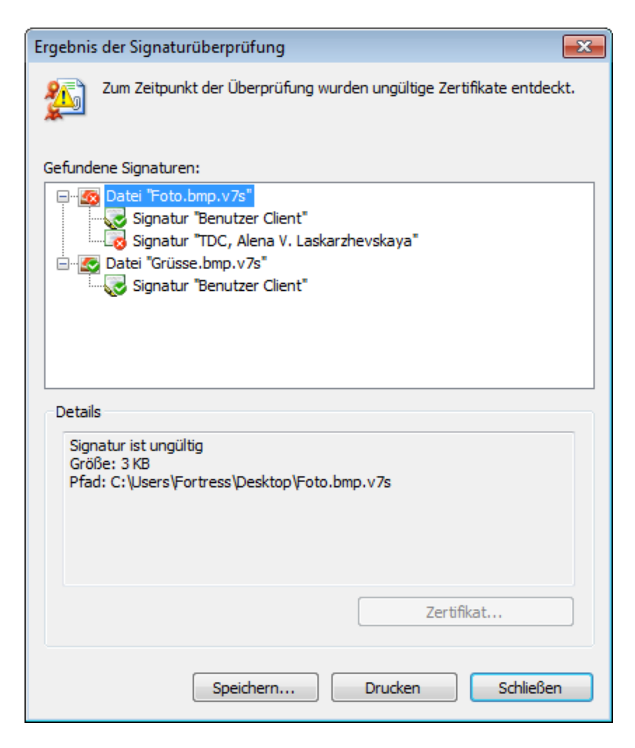


Abbildung 19. Signaturen mehrerer Dateien überprüfen

Im Fenster **Ergebnis der Signaturüberprüfung** sind alle gewählten Dateien und ihre digitalen Signaturen aufgeführt. Gültige Signaturen sind mit einem grünen Symbol gekennzeichnet, ungültige mit einem roten.



Hinweis. Wenn die Datei gleichzeitig eine angehängte und eine abgetrennte digitale Signatur besitzt, wird die abgetrennte Signatur im Fenster **Ergebnis der Signaturüberprüfung** nicht angezeigt.

Im Fenster **Ergebnis der Signaturüberprüfung** sind folgende Aktionen möglich:

- Wählen Sie im Bereich **Gefundene Signaturen** eine Datei oder eine digitale Signatur aus, um Informationen über diese Datei oder Signatur zu erhalten. Die Dateiinformation wird im Bereich **Details** eingeblendet.
- Wählen Sie im Bereich **Gefundene Signaturen** eine digitale Signatur aus und klicken Sie auf die Schaltfläche **Zertifikat**, um das Zertifikat zu sehen, mit dem die Datei signiert wurde.

Digitale Dateisignatur löschen

Führen Sie die folgenden Schritte aus, um die digitale Signatur einer Datei zu löschen:

1. Klicken Sie im ViPNet Business Mail Hauptfenster im Menü **Datei** auf den Eintrag **Datei signieren**, dann wählen Sie **Signatur entfernen**.
2. Geben Sie im Fenster **Öffnen** eine oder mehrere Dateien an, die angehängte oder abgetrennte digitale Signaturen besitzen (zum Beispiel `Document.txt.v7s` oder `Document.txt`, aber nicht `Document.txt.p7s`).
3. Klicken Sie auf die Schaltfläche **Öffnen**. Die digitalen Signaturen der gewählten Dateien werden gelöscht.



Hinweis. Wenn die Datei gleichzeitig eine angehängte und eine abgetrennte digitale Signatur besitzt, wird nur die angehängte Signatur entfernt.

Nachrichten ver- und entschlüsseln

Standardmäßig ist in „Business Mail“ das automatische Verschlüsseln von ausgehenden Nachrichten und Anhängen voreingestellt. Diese Einstellungen können geändert werden (s. Nachrichtenparameter einstellen auf S. 109).

Führen Sie die folgenden Schritte aus, um eine oder mehrere Nachrichten zu ver- oder entschlüsseln:

1. Wählen Sie im ViPNet Business Mail Hauptfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) eine oder mehrere Nachrichten in der Liste aus, die ver– oder entschlüsselt werden sollen.
2. Führen Sie einen der folgenden Schritte aus, um die gewählten Nachrichten zu verschlüsseln:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Verschlüsseln** .
   - Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen im Kontextmenü den Eintrag **Verschlüsseln**.

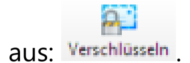
   Die gewählten Nachrichten werden mitsamt ihren Anhängen verschlüsselt.
3. Führen Sie einen der folgenden Schritte aus, um die gewählten Nachrichten zu entschlüsseln:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Entschlüsseln** .
   - Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen im Kontextmenü den Eintrag **Entschlüsseln**.

   Die gewählten Nachrichten werden mitsamt ihren Anhängen entschlüsselt.

Führen Sie folgende Schritte aus, um eine Nachricht zu ver– oder entschlüsseln, die im Fenster zum Anzeigen und verfassen von Nachrichten (auf S. 40) geöffnet ist:

1. Erstellen Sie eine neue Nachricht (s. Verfassen der Nachricht auf S. 42) oder öffnen eine ungesendete Nachricht in einem separaten Fenster.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Verschlüsseln** , um die Nachricht zu ver- oder entschlüsseln.

   Wenn die Nachricht verschlüsselt ist, sieht die Schaltfläche **Verschlüsseln** folgendermaßen aus: 
   .

   Wenn die Nachricht nicht verschlüsselt ist, sieht die Schaltfläche **Verschlüsseln** folgendermaßen aus: 
   .

5

Autoprocessing

Das Prinzip von Autoprocessing

Die automatische Verarbeitung von Nachrichten und Dateien in Übereinstimmung mit vordefinierten Regeln wird als Autoprocessing bezeichnet.

Die Autoprocessing-Regeln werden in drei Kategorien unterteilt:

- Verarbeitungsregeln für ausgehende Dateien.

  Diese Regeln sind dafür vorgesehen, Dateien mit einer bestimmten Maske für den Namen, die sich im angegebenen Ordner befinden, automatisch an einen oder mehrere Benutzer des ViPNet Netzwerks zu versenden. Es kann z.B. eine Regel konfiguriert werden, um Dateien mit dem Wort „Bericht" in ihrem Namen aus dem angegebenen Ordner an einen Kollegen, der Berichte überprüft, zu versenden.

- Verarbeitungsregeln für BML-Dateien.

  Diese Regeln sind dafür vorgesehen, Nachrichten mit einer bestimmten Maske für den Namen, die sich im angegebenen Ordner befinden, als Dateien im programminternen Format von ViPNet Business Mail automatisch von einem bestimmten Benutzer des Netzwerkknotens an einen oder mehrere Empfänger zu versenden. Mit Hilfe dieser Regeln kann der Austausch von Nachrichten mit den Benutzern eines ViPNet Netzwerks, mit dem keine Partnernetzwerk-Verbindung hergestellt wurde, eingerichtet werden. Dazu muss ein gesonderter Netzwerkknoten, über den Nachrichten an Sie weitergeleitet werden, in Ihrem Netzwerk erstellt und Verarbeitungsregeln für ausgehende BML-Dateien auf diesem Knoten konfiguriert werden. Für nähere Informationen siehe den Abschnitt Kommunikation mit Benutzern eines anderen ViPNet Netzwerks (auf S. 83).

- Verarbeitungsregeln für eingehende Nachrichten.

  Diese Regeln sind dafür vorgesehen, eingehende den angegebenen Parametern entsprechende Nachrichten auf eine der folgenden Weisen zu verarbeiten:

  - In den ViPNet Business Mail Ordner verschieben. Sie können so eine Regel konfiegurieren, um z.B. die von einem bestimmten Kollegen erhaltenen Nachrichten in einen bestimmten Ordner zu verschieben.
  - In den Ordner auf dem Laufwerk im BML-Format kopieren. Mit Hilfe dieser Regeln kann der Austausch von Nachrichten mit den Benutzern eines ViPNet Netzwerks, mit dem keine Partnernetzwerk-Verbindung hergestellt wurde, eingerichtet werden. Dazu muss ein gesonderter Netzwerkknoten, über den Nachrichten an Sie weitergeleitet werden, in Ihrem Netzwerk erstellt und Verarbeitungsregeln für ausgehende BML-Dateien auf diesem Knoten konfiguriert werden. Für nähere Informationen siehe den Abschnitt Kommunikation mit Benutzern eines anderen ViPNet Netzwerks (auf S. 83).
  - Nachricht und Anhänge in den Ordner auf dem Laufwerk kopieren. Sie können so eine Regel konfigurieren, um z.B. Nachrichten mit dem Wort „Bericht" in ihrem Namen, die Sie von bestimmten Kollegen erhalten, in einen bestimmten Ordner zu kopieren.

  Auch ein automatisches Versenden von Empfangsbestätigungen ist möglich.

Die Regeln von Autoprocessing können im Fenster Einstellungen im Bereich **Autoprocessing** (s. Autoprocessing–Regeln einstellen auf S. 85) erstellt werden.

Die Funktionsweise von Autoprocessing ist in der nachfolgenden Abbildung dargestellt:

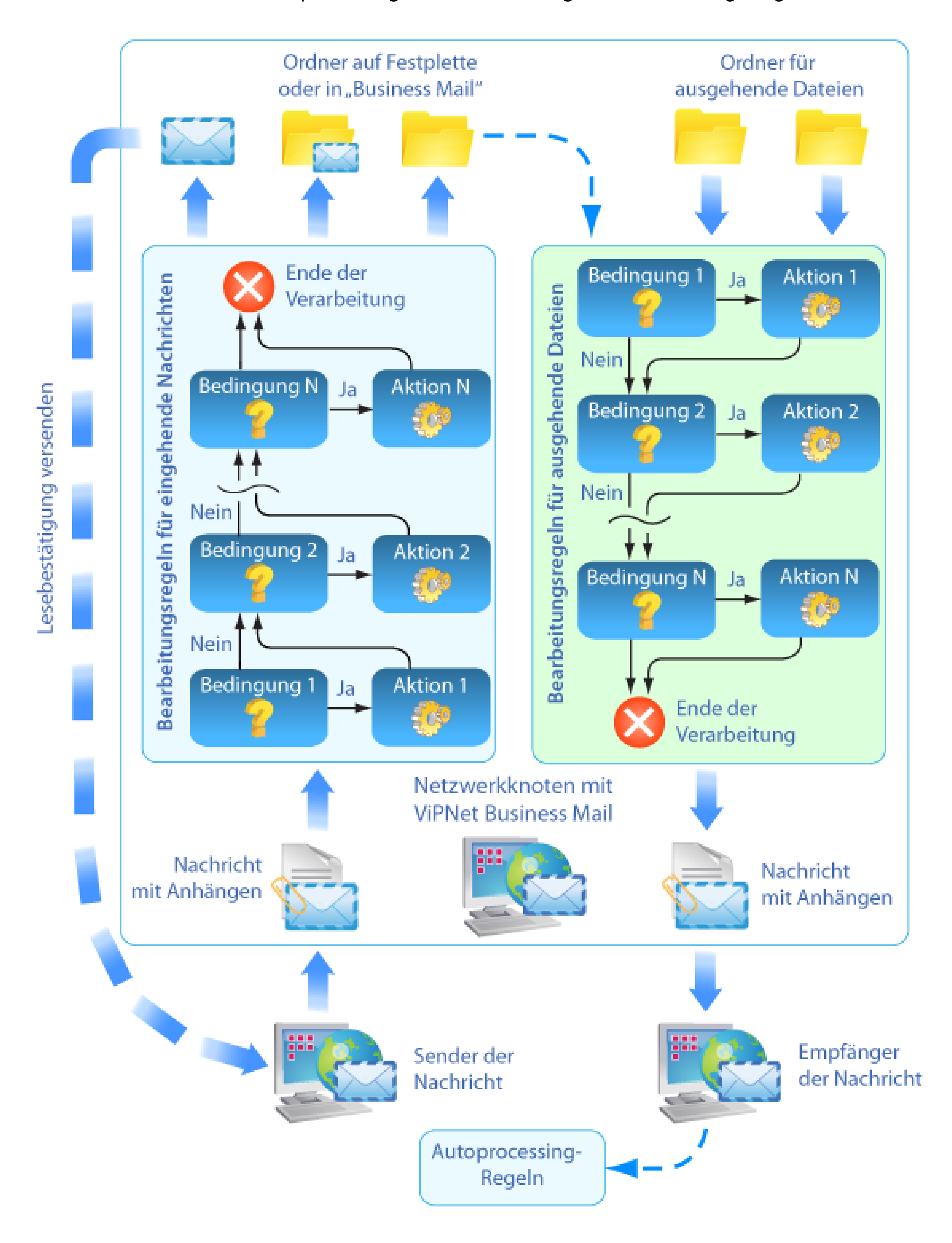


Abbildung 20. Die Funktionsweise von Autoprocessing

Die Verarbeitung von Nachrichten und Dateien wird folgendermaßen abgewickelt:

1. Das Programm "Business Mail" empfängt eine neue Nachricht oder legt im vordefinierten Ordner für ausgehende Dateien eine Datei ab. Ordner werden regelmäßig auf Vorliegen von Dateien geprüft.
2. Die Verarbeitung der Nachricht oder Datei in Übereinstimmung mit den entsprechenden Regeln des Autoprocessing wird begonnen. Die Verarbeitung erfolgt entsprechend der Reihenfolge von Regeln (Regelliste im Bereich **Autoprocessing**).
3. Jede Regel des Autoprocessing setzt sich aus einer Bedingung und einer Aktion zusammen. Wenn eine Nachricht oder Datei die Regelbedingung erfüllt, dann:
   - Wird die vordefinierte Aktion ausgeführt.
   - Wenn die Regelaktion keinen Abbruch der Weiterverarbeitung vorsieht, wird die Nachricht oder Datei von der nachfolgenden Regel bearbeitet.
4. Die Verarbeitung einer Nachricht oder Datei wird nach Prüfung aller Regeln oder nach einer Aktion, die einen Abbruch der Bearbeitung vorsieht, beendet.

Hinweis. Beim Versuch, Systemdateien oder Dateien mit Attribut „Schreibgeschützt" oder „Versteckt" zu verarbeiten, tritt ein Autoprocessing–Fehler auf. Das Programm sendet die Nachricht nicht ab, sondern schlägt für die aktuelle Sitzung von ViPNet Business Mail ein Abschalten der Regel vor, deren Ausführung zum Fehler geführt hat. Beim Klicken auf **Ja** wird diese Regel deaktiviert. Beim Klicken auf **Nein** oder bei Inaktivität von mehr als 20 Sekunden wird die Regel nicht deaktiviert, das Programm wird aber nicht mehr versuchen,diese Datei zu versenden. Beim Neustart wird das Programm ViPNet Business Mail in jedem Fall noch einmal versuchen, die Datei, die den Fehler verursacht hat, zu versenden.

Kommunikation mit Benutzern eines anderen ViPNet Netzwerks

Mit Hilfe der Autoprocessing-Regeln für die Verarbeitung von Dateien im programminternen Format von ViPNet Business Mail kann der Austausch von Nachrichten mit Benutzern eines ViPNet Netzwerks, mit dem keine Partnernetzwerk-Verbindung hergestellt wurde, konfiguriert werden.

Auf dem folgenden Schema finden Sie ein Beispiel dazu, wie die Weiterleitung von Nachrichten vom Benutzer „A“ eines ViPNet Netzwerks an den Benutzer „B“ eines anderen ViPNet Netzwerks hergestellt wird:

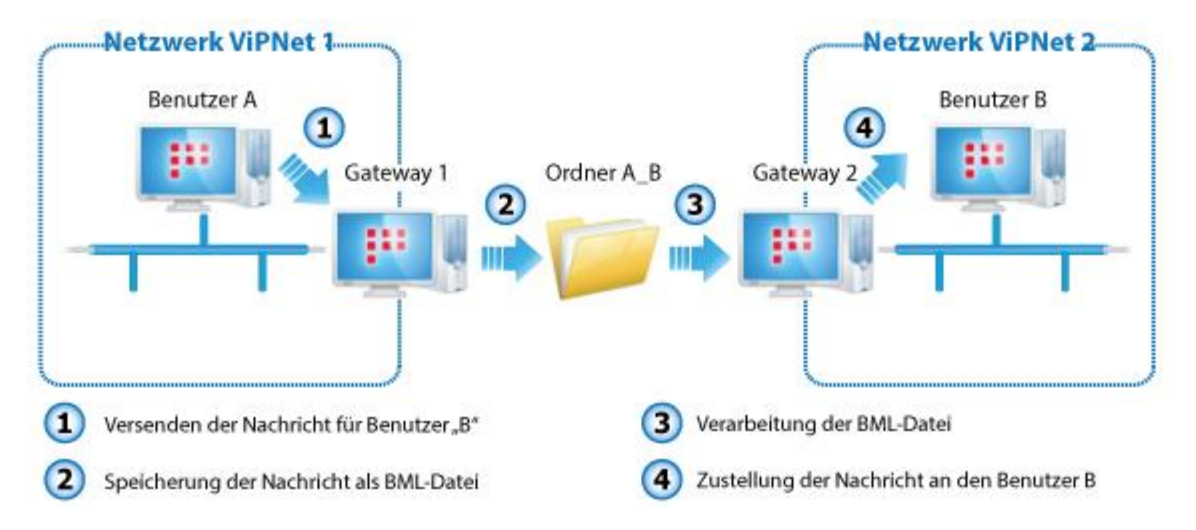


Abbildung 21. Herstellung des Austauschs von Nachrichten zwischen den Benutzern der miteinander nicht verbundenen ViPNet Netzwerke

Der Netzwerkadministrator des Absenders soll einen Knoten („Gateway 1“) zu seinem Netzwerk hinzufügen und einen Benutzer auf diesem Knoten einrichten, dieser Benutzer wird als Vertreter des Empfängers („B“) im Netzwerk ViPNet 1 fungieren. Der Benutzer „A“ wird Nachrichten an den Vertreter des Benutzers „B“ in seinem eigenen Netzwerk zum Zwecke der Weiterleitung an den Benutzer „B“ in ein anderes Netzwerk senden. Der Netzwerkadministrator des Empfängers soll einen Knoten („Gateway 2“) zu seinem Netzwerk hinzufügen und einen Benutzer auf diesem Knoten einrichten, dieser Benutzer wird als Vertreter des Absenders („A“) im Netzwerk ViPNet 2 fungieren. Der Vertreter des Benutzers „A“ wird die vom Vertreter des Benutzers „B“ erhaltenen Nachrichten an den Benutzer „B“ automatisch weiterleiten.



Hinweis. Ist es erforderlich, den Austausch von Nachrichten mit mehreren Benutzern aus einem anderen ViPNet Netzwerk herzustellen, sollen Vertreter für jeden Benutzer auf dem Knoten, der als Gateway im Netzwerk fungiert, eingerichtet werden.

Zur Weiterleitung von Nachrichten zwischen den Netzwerken sollen die Netzwerkadministratoren insgesamt min. 2 GB Speicherplatz zu Verfügung stellen, dort einen Ordner („A_B“) anlegen und die Speicherung von Daten durch die Knoten „Gateway 1“ und „Gateway 2“ in diesem Ordner erlauben.

Damit die Weiterleitung von Nachrichten vom Benutzer „A“ an den Benutzer „B“ über Vertreter automatisch erfolgt, sollen die Administratoren auf den Knoten „Gateway 1“ und „Gateway 2“ das Programm ViPNet Business Mail installieren und die Autoprocessing-Regeln folgenderweise konfigurieren:

- auf dem Knoten „Gateway 1“ werden Nachrichten vom Benutzer „A“ an den Vertreter des Benutzers „B“ im BML-Format in den Ordner „A_B“ kopiert (für nähere Informationen siehe den Abschnitt Regeln für eingehende Nachrichten erstellen (auf S. 92)).
- auf dem Knoten „Gateway 1“ werden BML-Dateien aus dem Ordner „A_B“ vom Vertreter des Benutzers „A“ an den Benutzer „B“ weitergeleitet (für nähere Informationen siehe den Abschnitt Erstellung einer Regel für BML-Dateien (auf S. 89)). Ist es beim Nachrichtenaustausch nicht erforderlich oder nicht möglich, die digitale Signatur zu überprüfen, aktivieren Sie das Entfernen von Signaturen in der Regel für eingehende Nachrichten.

Als Folge wird der folgende Algorithmus für den Austausch von Nachrichten zwischen den Benutzern „A“ und „B“ implementiert:

1. Im Netzwerk ViPNet 1 sendet der Benutzer „A“ eine Nachricht an den Vertreter des Benutzers „B“.
2. Auf dem Knoten „Gateway 1“ wird die Nachricht vom Benutzer „A“ durch die Autoprocessing-Regel für eingehende Nachrichten verarbeitet und als Datei `<Absender>_to_<Empfänger>_no_<Registrierungsnummer>.bml` im für den Knoten „Gateway 2“ zugänglichen Ordner „A_B“ gespeichert.
3. Auf dem Knoten „Gateway 2“ wird die im Ordner „A_B“ gespeicherte Nachrichtendatei durch die Autoprocessing-Regel für BML-Dateien verarbeitet und im Netzwerk ViPNet 2 vom Vertreter des Benutzers „A“ an den Benutzer „B“ weitergeleitet.
4. Der Benutzer „B“ erhält die Nachricht vom Vertreter des Benutzers „A“.

Damit der Benutzer „B“ Antworten an den Benutzer „A“ senden kann, sollen die Autoprocessing-Regel für eingehende Nachrichten auf dem Knoten „Gateway 2“ und die Verarbeitungsregel für eigehende Nachrichten auf dem Knoten „Gateway 1“ analog konfiguriert werden.

Autoprocessing–Regeln einstellen

Führen Sie die folgenden Schritte aus, um die Regeln für das Autoprocessing einzustellen:

1. Wählen Sie im ViPNet Business Mail Programmfenster im Menü **Extras** den Eintrag **Einstellungen** aus.
2. Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Autoprocessing** aus.

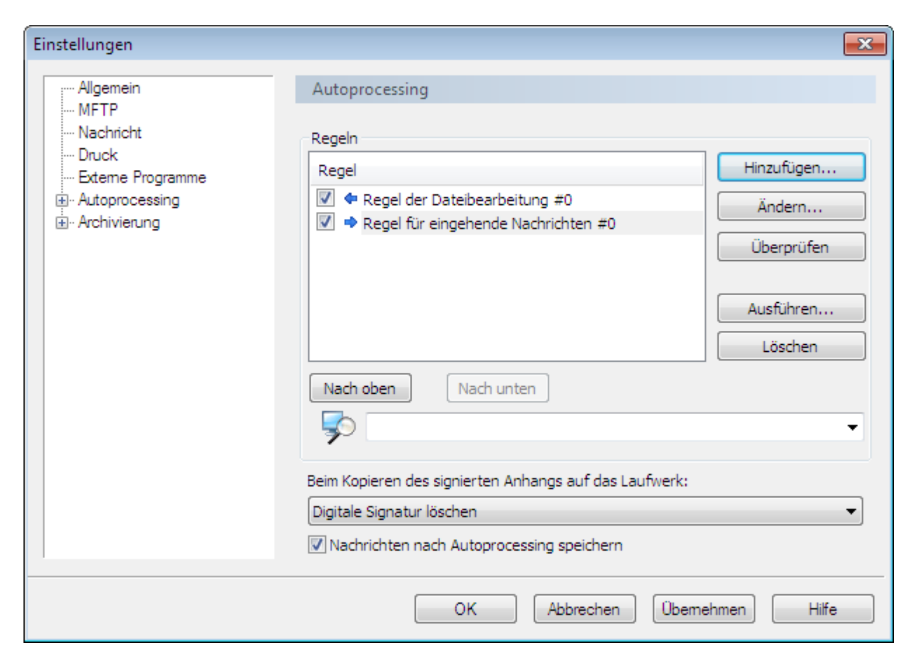


Abbildung 22. Autoprocessing–Parameter einstellen

3. Folgen Sie den Anweisungen eines der folgenden Abschnitte, um eine Regel der Dateiverarbeitung zu konfigurieren:
   - Regeln für ausgehende Dateien erstellen (auf S. 86).
   - Erstellung einer Regel für BML-Dateien (auf S. 89).
   - Regeln für eingehende Nachrichten erstellen (auf S. 92).
4. Geben Sie in der Suchzeile unterhalb der Liste einen Teil des Regelnamens an, um Regeln in der Liste zu suchen.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen vor dem Namen einer Regel in der Liste, um diese Regel ein– oder auszuschalten.
6. Wählen Sie eine Regel aus und verschieben diese mit Hilfe der Schaltflächen **Nach oben** und **Nach unten**, um die Reihenfolge der Regeln in der Liste zu ändern.



Hinweis. Die Verarbeitung von Nachrichten und Dateien erfolgt beim Autoprocessing entsprechend der Reihenfolge der Regeln in der Liste.

7. Die Konfiguration der Regeln ist in den folgenden Abschnitten beschrieben:

- Regeln für ausgehende Dateien erstellen (auf S. 86).
- Erstellung einer Regel für BML-Dateien (auf S. 89).
- Regeln für eingehende Nachrichten erstellen (auf S. 92).

8. Wählen Sie eine Regel in der Liste aus und klicken auf **Überprüfen**, um die Richtigkeit der Regelparameter zu prüfen. Das Programm gibt eine Meldung mit dem Prüfergebnis aus.
9. Wählen Sie eine Regel in der Liste aus und klicken auf **Ausführen**, um die Bearbeitung der eingehenden Nachrichten durch diese Regel manuell zu starten.

   Nachrichten, die sich im Ordner **Posteingang** befinden, werden durch die gewählte Regel verarbeitet. Ein manueller Start der Bearbeitung kann zum Beispiel dazu verwendet werden, Nachrichten mit bestimmten Eigenschaften aus dem Ordner Posteingang in andere Ordner von „Business Mail" zu verschieben.
10. Wenn Sie eine Regel aus der Liste entfernen möchten, wählen Sie diese Regel in der Liste aus und klicken auf **Löschen**.
11. Wählen Sie den passenden Eintrag in der Liste **Beim Kopieren des signierten Anhangs auf dem Laufwerk** aus, um zu bestimmen, wie mit den digitalen Signaturen von auf die Festplatte kopierten Dateien zu verfahren ist.
12. Aktivieren oder deaktivieren Sie das entsprechende Kontrollkästchen, um zu bestimmen, ob Nachrichten nach dem Autoprocessing in den Ordnern von „Business Mail" erhalten bleiben oder gelöscht werden.

    Wenn das Kontrollkästchen deaktiviert ist, werden die verarbeiteten Nachrichten automatisch gelöscht. Informationen über diese Nachrichten werden im Ordner **Audit** gespeichert. Für nähere Informationen über die Parametereinstellung zur Speicherung von Informationen im Ordner **Audit** siehe den Abschnitt Zusätzliche Möglichkeiten und Parameter des Programms (auf S. 114).

Regeln für ausgehende Dateien erstellen

Führen Sie die folgenden Schritte aus, um eine Regel für die Bearbeitung ausgehender Dateien zu erstellen:

1. Wählen Sie im ViPNet Business Mail Programmfenster im Menü **Extras** den Eintrag **Einstellungen**.
2. Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Autoprocessing** (s. Abbildung auf S. 85).
3. Klicken Sie in der Registerkarte **Autoprocessing** auf die Schaltfläche **Hinzufügen**.

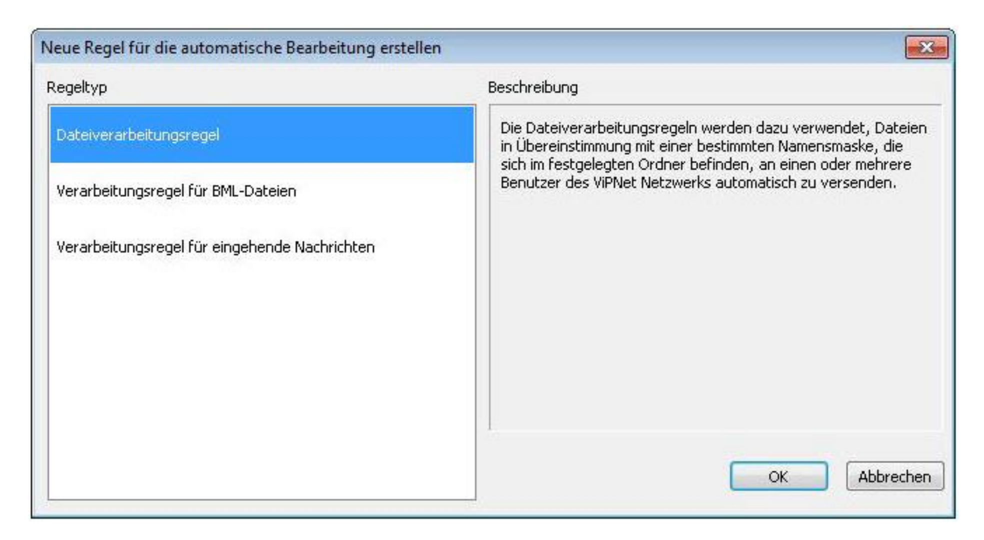


Abbildung 23. Regeltyp wählen

4 Wählen Sie im Fenster **Neue Regel für die automatische Bearbeitung erstellen** den Typ **Dateiverarbeitungsregel** und klicken auf **OK**.

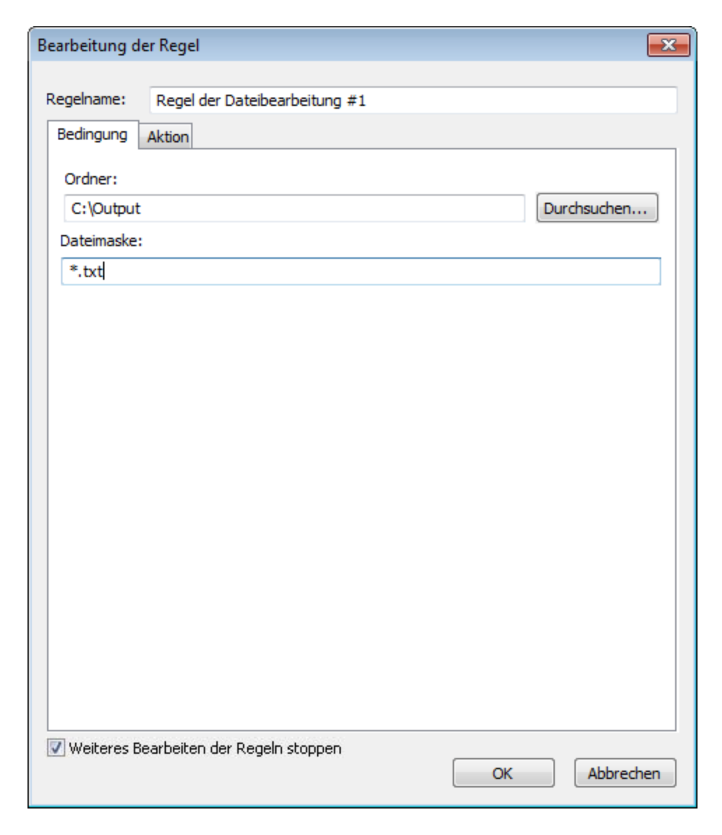


Abbildung 24. Bedingung einer Regel für die automatische Bearbeitung von Dateien

5 Geben Sie im Fenster **Bearbeitung einer Regel** im Feld **Regelname** einen Namen für die neue Regel ein.

6 Klicken Sie in der Registerkarte **Bedingung** auf die Schaltfläche **Durchsuchen** und wählen im Fenster **Durchsuchen** einen Ordner aus, in dem die ausgehenden Dateien abgelegt werden.

7 Geben Sie im Feld **Dateimaske** die Maske für den Namen der Datei an, die von der neuen Regel verarbeitet werden soll.

Bei der Definition der Maske wird die Groß- und Kleinschreibung ignoriert, und es können folgende Sonderzeichen verwendet werden:

- * – entspricht einer Reihenfolge beliebiger Zeichen.
- ? – entspricht genau einem beliebigen Zeichen.

8 Öffnen Sie die Registerkarte **Aktion**.

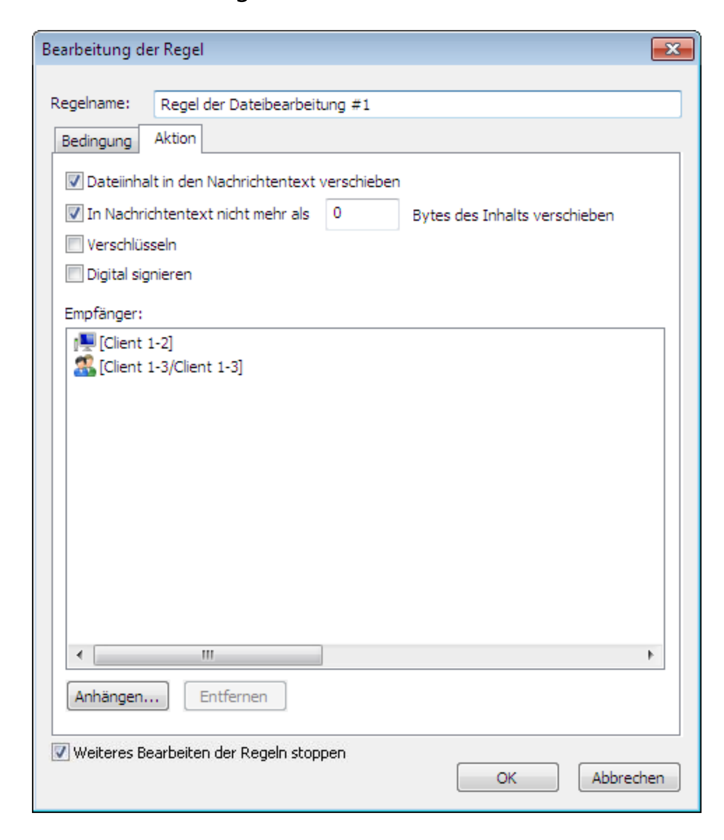


Abbildung 25. Aktion einer Regel für die automatische Bearbeitung von Dateien

9 Wenn der Dateiinhalt in den Nachrichtentext übernommen werden soll, aktivieren Sie das entsprechende Kontrollkästchen. Dabei wird das Kästchen **In Nachrichtentext nicht mehr als ... Bytes des Inhalts verschieben** wieder aktiv.



Achtung! Es wird empfohlen, dieses Kontrollkästchen nur für die Bearbeitung von Textdateien, das heißt Dateien vom Format TXT, zu aktivieren. Wenn diese Funktion für Dateien anderer Formate genutzt wird, dann wird in den Nachrichtentext eine unleserliche Folge von Zeichen eingefügt.

Das Kontrollkästchen **In Nachrichtentext nicht mehr als ... Bytes des Inhalts** wirkt folgendermaßen:

- Wenn das Kontrollkästchen deaktiviert ist (standardmäßig der Fall), wird der Dateiinhalt zur Gänze in den Nachrichtentext eingefügt.
- Aktivieren Sie das Kontrollkästchen **In Nachrichtentext nicht mehr als ...**, um einen Teil der Datei in den Nachrichtentext zu übernehmen. Geben Sie im Textfeld die Anzahl der Bytes an, die eingefügt werden soll.

Wenn die Größe der Datei die angegebene Anzahl der Bytes übersteigt, wird ein Teil der Datei in den Nachrichtentext eingefügt, und die Datei selbst als Anlage an die Nachricht angehängt.

10 Aktivieren Sie das Kontrollkästchen **Verschlüsseln**, um die Nachricht zu verschlüsseln.

11 Aktivieren Sie das Kontrollkästchen **Digital signieren**, um die Nachricht mit einer digitalen Signatur zu versehen.

12 Klicken Sie auf die Schaltfläche **Hinzufügen**, um Empfänger, an die die Datei gesendet wird, hinzuzufügen, und wählen einen oder mehrere Empfänger mit Hilfe der Schaltfläche **Auswählen** aus dem Adressbuch aus. Klicken Sie danach auf die Schaltfläche **Schließen**.

Zum Entfernen der Empfänger wählen Sie einen oder mehrere Empfänger in der Liste aus und klicken auf die Schaltfläche **Entfernen**.

13 Deaktivieren Sie das Kontrollkästchen **Weiteres Bearbeiten der Regeln stoppen** (standardmäßig aktiviert), wenn nach Abschluss der Bearbeitung durch die aktuelle Regel eine Bearbeitung der Datei durch nachfolgende Regeln erforderlich ist.

14 Klicken Sie auf **OK**, um die Regel zu speichern.

Erstellung einer Regel für BML-Dateien

Führen Sie folgende Schritte aus, um eine Verarbeitungsregel für Dateien im programminternen Format von ViPNet Business Mail zu erstellen:

1 Wählen Sie den Eintrag **Einstellungen** im Programmfenster ViPNet Business Mail im Menü **Extras**.

2 Wählen Sie den Bereich **Autoprocessing** **(s. Abbildung auf S. 85)** im Fenster **Einstellungen** in der Navigationsleiste.

3 Klicken Sie auf die Schaltfläche **Hinzufügen** in der Registerkarte **Autoprocessing**.

4 Wählen Sie den Regeltyp **Verarbeitungsregel für BML-Dateien** im Fenster **Neue Regel für die automatische Bearbeitung erstellen** und klicken auf **OK**.

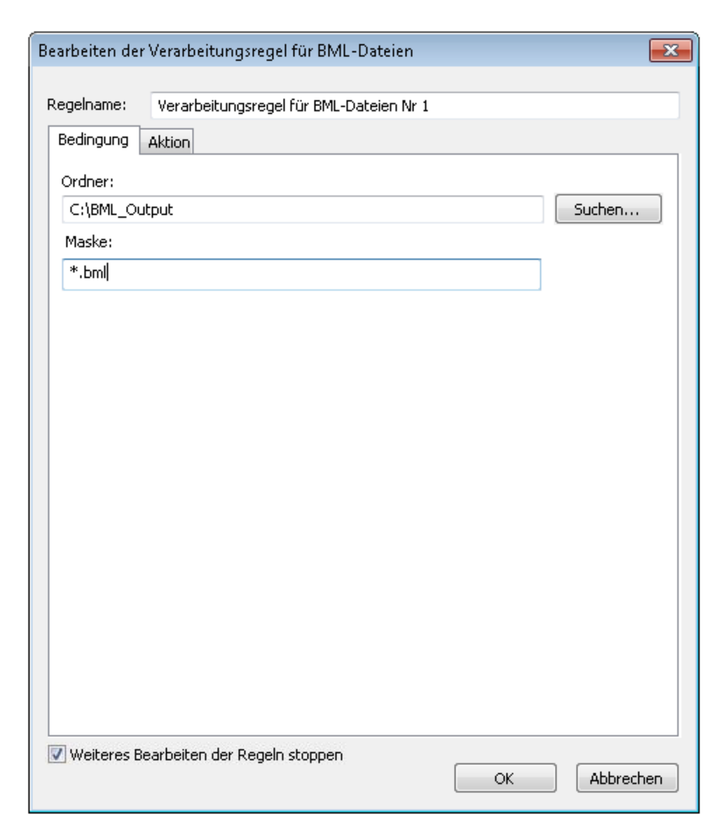


Abbildung 26. Bedingung für die Verarbeitungsregel für BML-Dateien

5 Geben Sie einen Namen für die zu erstellende Regel im Feld **Regelname** im Fenster **Bearbeiten der Verarbeitungsregel für BML-Dateien** ein.

6 Klicken Sie in der Registerkarte **Bedingung** auf die Schaltfläche **Suchen** und wählen im Fenster **Ordner durchsuchen** einen Ordner aus, in dem die ausgehenden Dateien abgelegt werden.

Geben Sie im Feld **Maske** die Maske für den Namen der BML-Datei ein, die von der zu erstellenden Regel verarbeitet werden soll.

Bei der Definition der Maske werden Groß- und Kleinbuchstaben ignoriert, dabei dürfen folgende Sonderzeichen verwendet werden:

- * — entspricht einer Reihenfolge beliebiger Zeichen.
- ? — entspricht einem beliebigen Zeichen.

Standardmäßig wird die Maske `*.bml` verwendet, d.h. alle BML-Dateien werden von dieser Regel verarbeitet.

7 Öffnen Sie die Registerkarte **Aktion**.

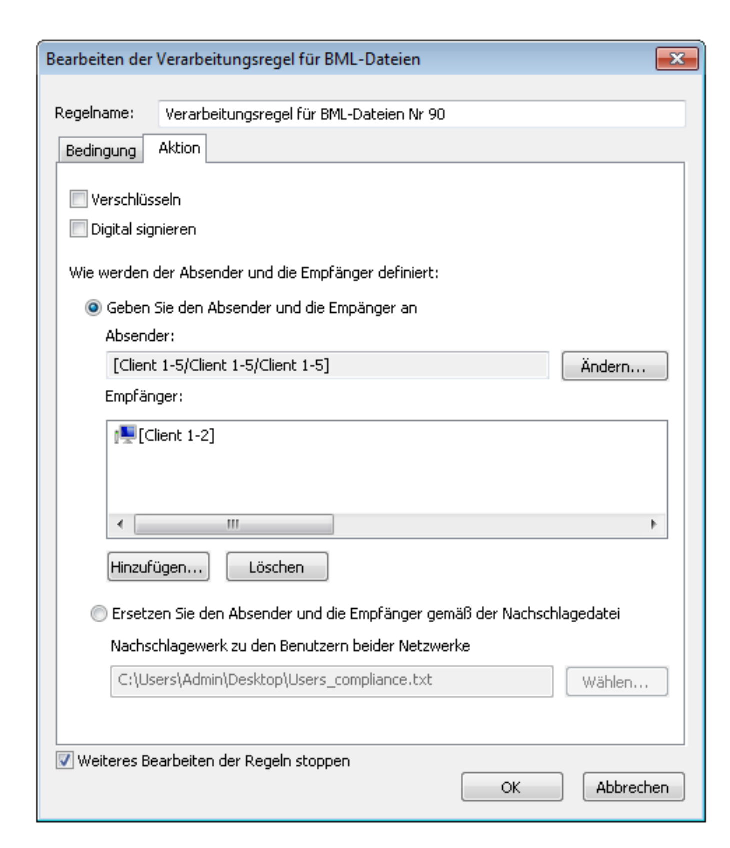


Abbildung 27. Aktion der Verarbeitungsregel für BML-Dateien

8 Aktivieren Sie das Kontrollkästchen **Verschlüsseln**, um die Nachricht zu verschlüsseln.

9 Aktivieren Sie das Kontrollkästchen **Digital signieren**, um die Nachricht mit einer digitalen Signatur zu versehen.

10 Legen Sie fest, wie der Absender und die Empfänger definiert werden:

- Sollen Nachrichten von einem bestimmten Absender oder für bestimmte Empfänger, die manuell eingegeben werden, verarbeitet werden, aktivieren Sie das Kontrollkästchen **Geben Sie den Absender und die Empfänger an**.

  Im Feld **Absender** ist standardmäßig der aktuelle Benutzer des Netzwerkknotens gewählt. Wählen Sie bei Bedarf einen anderen Benutzer aus dem Adressbuch aus, indem Sie auf die Schaltfläche **Ändern** klicken. Es kann nur ein Absender gewählt werden.

  Um Empfänger, an die die Datei gesendet wird, hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen einen oder mehrere Benutzer aus dem Adressbuch mit Hilfe der Schaltfläche **Wählen** aus. Klicken Sie dann auf die Schaltfläche **Schließen**.

  Um Empfänger zu entfernen, wählen Sie einen oder mehrere Empfänger aus der Liste aus und klicken auf die Schaltfläche **Löschen**.

- Sollen der Absender und die Empfänger automatisch eingesetzt werden, aktivieren Sie das Kontrollkästchen **Ersetzen Sie den Absender und Empfänger gemäß der Nachschlagedatei**. Danach geben Sie mit Hilfe der Schaltfläche **Wählen** an, wo sich die Datei mit Übereinstimmungen zwischen Benutzern beider ViPNet Netzwerke befindet.

  Diese Möglichkeit wird dann genutzt, wenn Nachrichten zwischen Benutzern eines ViPNet Netzwerks, mit dem keine Partnernetzwerk-Verbindung hergestellt wurde, ausgetauscht werden

sollen. In der Datei mit Benutzerübereinstimmungen, welche eine Textdatei darstellt, wird die Übereinstimmung zwischen Benutzern des fremden Netzes und ihren Vertretern im eigenen Netz festgelegt (s. Kommunikation mit Benutzern eines anderen ViPNet Netzwerks auf S. 83).

11 Deaktivieren Sie das Kontrollkästchen **Weiteres Bearbeiten der Regeln stoppen** (standardmäßig aktiviert), wenn nach Abschluss der Dateiverarbeitung durch die aktuelle Regel eine Dateiverarbeitung durch weitere Regeln erforderlich ist.

12 Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

Regeln für eingehende Nachrichten erstellen

Führen Sie folgende Schritte aus, um eine Regel für die Bearbeitung eingehender Nachrichten zu erstellen:

1 Wählen Sie im ViPNet Business Mail Programmfenster im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Autoprocessing** (s. Abbildung auf S. 85).

3 Klicken Sie in der Registerkarte **Autoprocessing** auf die Schaltfläche **Hinzufügen**.

4 Wählen Sie im Fenster **Neue Regel für die automatische Bearbeitung erstellen** den Typ **Verarbeitungsregel für eingehende Nachrichten** und klicken auf **OK**.

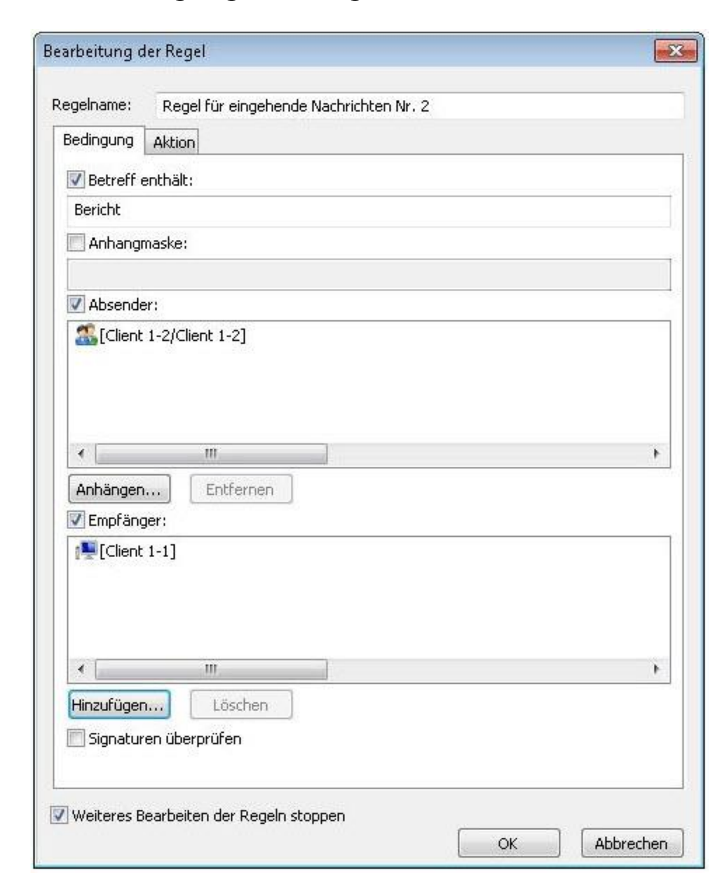


Abbildung 28. Bedingung einer Regel für die automatische Bearbeitung von Nachrichten

5 Geben Sie im Fenster **Bearbeitung der Regel** im Feld **Regelname** einen Namen für die neue Regel ein.

6 Geben Sie in der Registerkarte **Bedingung** die Bedingungen an, bei deren Erfüllung die Nachricht durch die aktuelle Regel bearbeitet wird.

- Aktivieren Sie das Kontrollkästchen **Betreff enthält**, um Nachrichten zu bearbeiten, deren Betreff eine bestimmte Folge von Zeichen enthält. Geben Sie im Feld unter dem Kästchen die erforderliche Zeichenfolge ein.
- Aktivieren Sie das Kontrollkästchen **Anhangmaske**, um Nachrichten mit Anhängen zu bearbeiten, deren Namen einer bestimmten Maske entsprechen. Geben Sie im Feld unter dem Kästchen die Maske für den Anlagennamen ein.

  Bei der Definition der Maske wird die Groß- und Kleinschreibung ignoriert, und es können folgende Sonderzeichen verwendet werden:

  - * – entspricht einer Reihenfolge beliebiger Zeichen.
  - ? – entspricht genau einem beliebigen Zeichen.

  Die Bedingung ist erfüllt, wenn der Name eines oder mehrerer Nachrichtenanhänge mit der definierten Maske übereinstimmt. Bei Erfüllung dieser Bedingung werden nur Anhänge verarbeitet, deren Namen der Maske entsprechen.

- Sollen Nachrichten von bestimmten Absendern oder Empfängern verarbeitet werden, aktivieren Sie das entsprechende Kontrollkästchen, klicken auf die Schaltfläche **Hinzufügen** und wählen einen oder mehrere Benutzer aus dem Adressbuch aus mit Hilfe der Schaltfläche **Auswählen**. Klicken Sie danach auf die Schaltfläche **Schließen**.

  Ist es erforderlich, Absender oder Empfänger zu entfernen, wählen Sie diese aus der jeweiligen Liste aus und klicken auf die Schaltfläche **Entfernen**.

  Für die Aktivierung der Bedingung ist erforderlich, dass der Absender oder der Empfänger der Nachricht einer der in dieser Liste angegebenen Benutzer ist.

- Wenn digitale Signaturen der Nachrichten überprüft werden sollen, dann aktivieren Sie das Kontrollkästchen **Signaturen überprüfen**.

  Damit die Bedingung erfüllt ist, sollten die Anhänge der Nachricht mit einer gültigen Signatur signiert sein.



Achtung! Wenn für die Regel mehrere Bedingungen angegeben wurden, wird die Nachricht nur bei gleichzeitiger Erfüllung aller Bedingungen bearbeitet.

---

7 Öffnen Sie die Registerkarte **Aktion**.

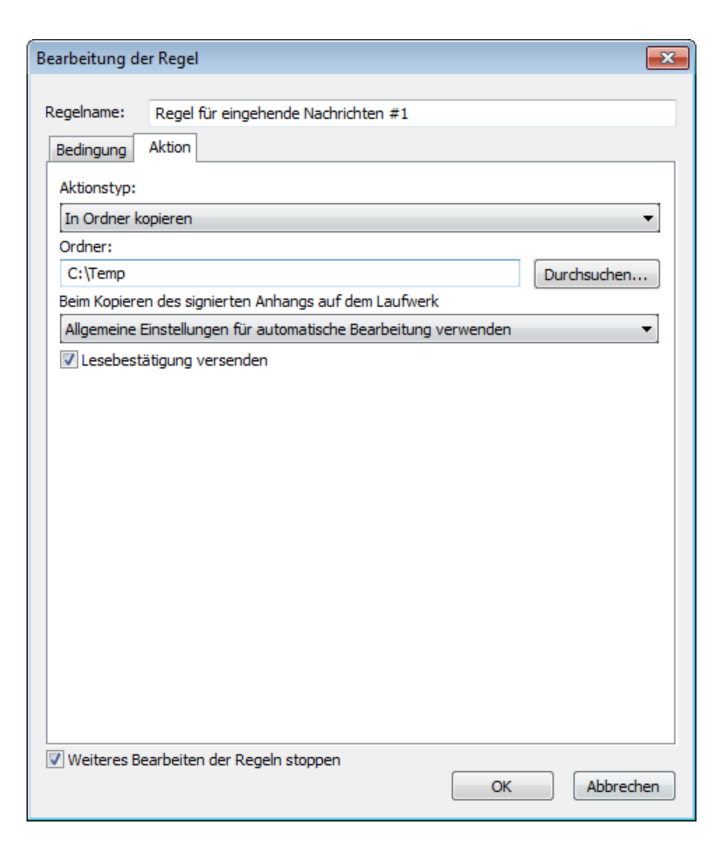


Abbildung 29. Aktion einer Regel für die automatische Bearbeitung von eingehenden Nachrichten

8 Wählen Sie in der Dropdownliste **Aktionstyp** einen der Einträge aus:

- **Speichern im Ordner auf Festplatte**.



Achtung! Ist das automatische Speichern von eingehenden Nachrichten in den Ordner auf dem Laufwerk konfiguriert, wird der neue Anhang nicht gespeichert, wenn eine Nachricht mit einem Anhang, dessen Name dem Namen einer in den Ordner zuvor kopierten Datei entspricht, verarbeitet wird.

- **Kopieren im BML-Format in einen Ordner auf Datenträger**.
- **Beim Speichern in den Ordner Dateien mit dem gleichen Namen überschreiben.** Bei Übereinstimmung der Dateinamen wird die Datei, die sich bereits im Ordner befindet, durch die Anlagendatei der bearbeiteten Nachricht ersetzt.
- **Beim Speichern in den Ordner ältere Dateien überschreiben.** Bei Übereinstimmung der Dateinamen wird die Datei, die sich bereits im Ordner befindet, durch die Anlagendatei nur dann ersetzt, wenn diese später modifiziert wurde.
- **Beim Speichern in den Ordner die kopierten Dateien umbenennen.** Bei Übereinstimmung der Dateinamen erhält die zu speichernde Anlagendatei den Postfix _copy<Kopienummer>.
- **In den Business Mail Ordner verschieben.**

Beim Speichern der Nachricht im BML-Format auf dem Laufwerk wird die Nachricht als die Datei <Absender>_to_<Empfänger>_no_<Registrierungsnummer>.bml im ausgewählten Ordner gespeichert. Ansonsten werden Anhänge und der Nachrichtentext beim Speichern der Nachricht auf

dem Laufwerk als Datei `BODY-<Registrierungsnummer>.rtf` oder `blank.txt` im ausgewählten Ordner gespeichert, wenn Sie mit Nachrichten ohne Formatierung arbeiten (s. Allgemeine Parameter einstellen auf S. 103). Enthält die Nachricht keinen Text, werden die RTF- und TXT-Dateien nicht erstellt.

9 Wenn das Kopieren von Nachrichten in einen Ordner auf der Festplatte gewählt wurde, führen Sie folgende Schritte aus:

   - Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen im Fenster **Durchsuchen** einen Ordner aus, in dem der Nachrichtentext und die Anhänge abgelegt werden sollen.
   - Wählen Sie in der Dropdownliste **Beim Kopieren des signierten Anhangs auf dem Laufwerk** einen Eintrag aus:
     - **Allgemeine Einstellungen für automatische Bearbeitung verwenden.** Bei der Auswahl dieser Option wird die im Bereich **Autoprocessing** voreingestellte Aktion ausgeführt (s. Autoprocessing–Regeln einstellen auf S. 85).
     - **Digitale Signatur löschen**.
     - **Digitale Signatur an Datei anhängen**.
     - **Digitale Signatur als externe Datei speichern**.

     Weitere Informationen über das Anhängen und Trennen von digitalen Signaturen finden Sie in Dateisignatur anhängen und abtrennen (auf S. 75).
   - Ist es erforderlich, Lesebestätigungen zu senden, wenn nur einige Anhänge verarbeitet wurden, aktivieren Sie das Kontrollkästchen **Lesebestätigung versenden**.



Hinweis. Nach der Verarbeitung der Nachricht mit allen Anhängen wird immer eine Bestätigung gesendet, unabhängig von den Einstellungen.

   - Wird das Kopieren der BML-Nachricht ausgewählt, aktivieren Sie bei Bedarf das Kontrollkästchen **Digitale Signatur aus ganzer Nachricht entfernen**. Die Nachricht wird in diesem Fall ohne digitale Signaturen gespeichert.

10 Ist die Verschiebung der Nachricht in den ViPNet Business Mail Ordner ausgewählt, klicken Sie auf die Schaltfläche **Durchsuchen** und wählen einen Ordner für die Speicherung von Nachrichten im Fenster **Ordner auswählen** aus. Das soll ein von Ihnen angelegter Unterordner im Ordner **Posteingang** oder **Business Mail** sein.

11 Deaktivieren Sie das Kontrollkästchen **Weiteres Bearbeiten der Regeln stoppen** (standardmäßig aktiviert), wenn nach Abschluss der Bearbeitung durch die aktuelle Regel eine Bearbeitung der Nachricht durch nachfolgende Regeln erforderlich ist.

12 Klicken Sie auf **OK**, um die Regel zu speichern.

Autoprocessing optimieren

Durch die Regeln von Autoprocessing wird in manchen Fällen eine sehr hohe Anzahl von Nachrichten verarbeitet. Die Bearbeitung sehr großer Mengen von Daten basierend auf Standardeinstellungen von Autoprocessing kann die Arbeit von ViPNet Business Mail bedeutend verlangsamen, den laufenden Empfang der Korrespondenz anhalten, unvorhergesehene Fehler hervorrufen.

Folgende Einstellungen sind empfohlen, um den Durchsatz großer Mengen an Nachrichten im Autoprocessing zu beschleunigen:

1. Melden Sie sich in ViPNet Business Mail als Administrator an (s. Arbeiten mit Administratorrechten auf S. 114).
2. Wählen Sie im Hauptfenster im Menü **Extras** den Eintrag **Einstellungen**.
3. Klicken Sie im Fenster **Einstellungen** in der Navigationsleiste auf den Bereich **Administrator**.
4. Deaktivieren Sie im Bereich **Administrator** das Kontrollkästchen **Einträge über die gelöschten Nachrichten im Ordner „Audit" speichern**.
5. Wählen Sie in der Navigationsleiste den Bereich **Autoprocessing**.
6. Deaktivieren Sie im Bereich **Autoprocessing** (s. Autoprocessing–Regeln einstellen auf S. 85) das Kontrollkästchen **Nachrichten nach Autoprocessing speichern**.

Diese Einstellungen erlauben es, die Geschwindigkeit der Nachrichtenverarbeitung durch die Regeln des Autoprocessing wesentlich zu erhöhen.



Achtung! Deaktivieren Sie die Speicherung von durch Autoprocessing verarbeiteten Nachrichten und von Einträgen über gelöschte Nachrichten im Ordner **Audit**, gehen die verarbeiteten Nachrichten mit nicht verarbeiteten Anhängen sowie die Informationen darüber verloren.

Autoprocessing–Logdatei anzeigen

Die Information über Ereignisse, die beim Autoprocessing auftreten, wird in der Logdatei von Autoprocessing erfasst. Die Einstellung der Parameter für die Logdatei wird weiter unten beschrieben (s. Logdatei–Parameter für Autoprocessing einstellen auf S. 100).

Führen Sie folgende Schritte aus, um die Logdatei anzuzeigen:

1 Wählen Sie im ViPNet Business Mail Hauptfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Datei** den Eintrag **Autoprocessing Logdatei**. Es wird das Fenster **Anzeige der Logdatei** eingeblendet.

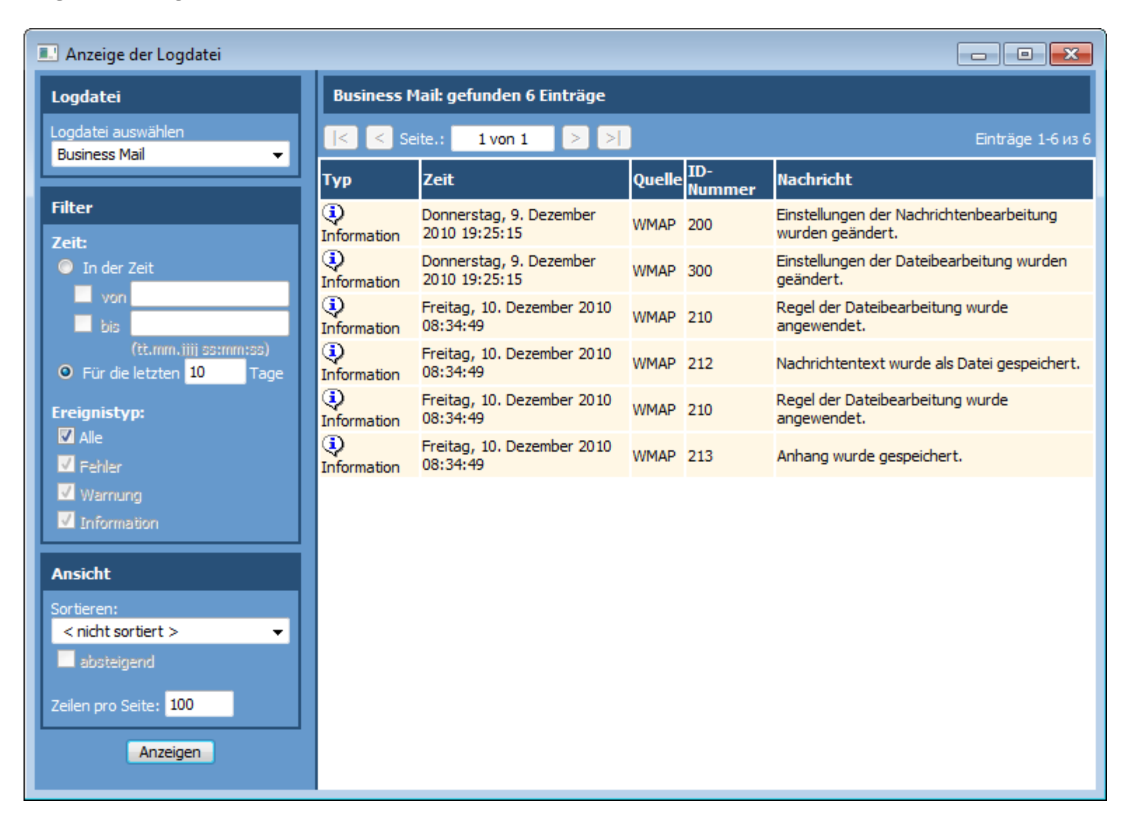


Abbildung 30. Autoprocessing–Logdatei anzeigen

2 Geben Sie im linken Fensterteil von **Anzeige der Logdatei** im Bereich **Filter** die Parameter für die Ereignissuche an:

- Geben Sie die Ereigniszeit auf eine der zwei Arten an:
  - Wählen Sie die Option **In der Zeit**, um nach Ereignissen zu suchen, die innerhalb eines bestimmten Zeitabschnitts aufgetreten sind. Um den Beginn und das Ende des Zeitabschnitts zu definieren, aktivieren Sie die entsprechende Kontrollkästchen (**von** und **bis**) und geben im Feld rechts davon das Datum und die Uhrzeit des Intervallbeginns im Format `tt.mm.jjjj hh:mm:ss` an.
  - Wählen Sie die Option **Für die letzten … Tage**, um nach Ereignissen zu suchen, die in den letzten Tagen aufgetreten sind.

  Standardmäßig ist die Ereignissuche für die letzten 10 Tage voreingestellt.

- Bestimmen Sie den Ereignistyp, indem Sie die Kontrollkästchen **Alle**, **Fehler**, **Warnung**, **Information** (de–)aktivieren. Standardmäßig wird nach allen Ereignistypen gesucht.

3 Im Bereich **Ansicht**:

- Wählen Sie in der Liste **Sortieren** die Reihenfolge der Sortierung aus. Standardmäßig ist der Eintrag **<nicht sortiert>** ausgewählt.
- Aktivieren Sie das Kontrollkästchen **absteigend**, um die Reihenfolge der Sortierung zu ändern (dieses Kontrollkästchen ist inaktiv, wenn in der Liste **Sortieren** der Eintrag **<nicht sortiert>** ausgewählt ist).
- Geben Sie im Feld **Zeilen pro Seite** die Anzahl von Ereignissen an, die auf einer Seite angezeigt werden sollen (standardmäßig 100).

4 Nachdem Sie alle Suchparameter eingestellt haben, klicken Sie auf die Schaltfläche **Anzeigen**. Im Ansichtsbereich des Fensters **Anzeige der Logdatei** wird eine Liste der gefundenen Ereignisse eingeblendet (s. Abbildung auf S. 97).

5 Wenn die Suchergebnisse auf mehreren Seiten aufgeführt sind, benutzen Sie für das Umschalten zwischen den Seiten die Schaltflächen oberhalb der Ergebnisliste.

6 Doppelklicken Sie auf ein Ereignis, um weitere Informationen darüber anzuzeigen. Es wird das Fenster **Information über das Ereignis** eingeblendet.

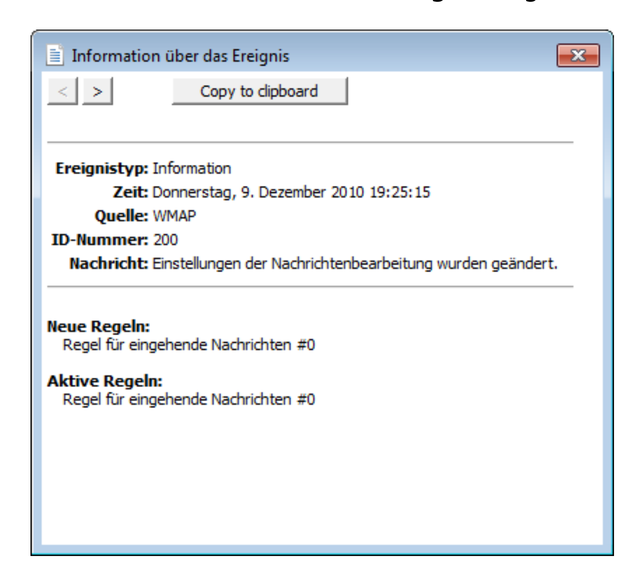


Abbildung 31. Ausführliche Information über ein Ereignis

Klicken Sie auf die Schaltfläche < im oberen Bereich des Fensters **Information über das Ereignis**, um zum vorhergehenden Ereignis in der Liste zu navigieren. Klicken Sie auf die Schaltfläche >, um zum nachfolgenden Ereignis zu gehen.

Ereignisse, die in der Logdatei registriert werden, sind in der folgenden Tabelle aufgeführt:

Ereignistyp	Ereignis–ID	Ereignisbeschreibung
Information	100	Einstellungen der Logdatei wurden geändert
	200	Einstellungen der Nachrichtenbearbeitung wurden geändert
	210	Regel der Dateibearbeitung wurde angewendet
	211	Nachricht wurde verschoben
	212	Nachrichtentext wurde als Datei gespeichert
	213	Anhang wurde gespeichert
	300	Einstellungen der Dateibearbeitung wurden geändert
	312	Automatische Dateibearbeitung neu gestartet
	321	Datei an die Nachricht angehängt
	322	Nachricht mit Anhang wurde gesendet
	400	Die Autoprocessing-Regeln für BML-Dateien wurden geändert.
Warnung	311	Automatische Dateibearbeitung angehalten
Fehler	1251	Fehler bei der Bearbeitung der Nachricht
	1252	Fehler bei der Suche der Regel
	1253	Fehler bei der Anwendung der Regel
	1254	Fehler bei der Verschiebung der Nachricht
	1255	Fehler beim Speichern der Nachricht
	1256	Fehler beim Speichern des Anhangs
	1351	Fehler bei der Dateisuche
	1352	Fehler bei der Bearbeitung der Datei
	1353	Fehler beim Anhängen der Datei
	1354	Fehler bei Versand der Nachricht mit Anhang

Logdatei–Parameter für Autoprocessing einstellen

Führen Sie folgende Schritte aus, um die Parameter für die Autoprocessing–Logdatei einzustellen:

1 Wählen Sie im ViPNet Business Mail Programmfenster im Menü **Extras** den Eintrag **Einstellungen**.

2 Klappen Sie in der Navigationsleiste des Fensters **Einstellungen** den Eintrag **Autoprocessing** > **Logdatei**.

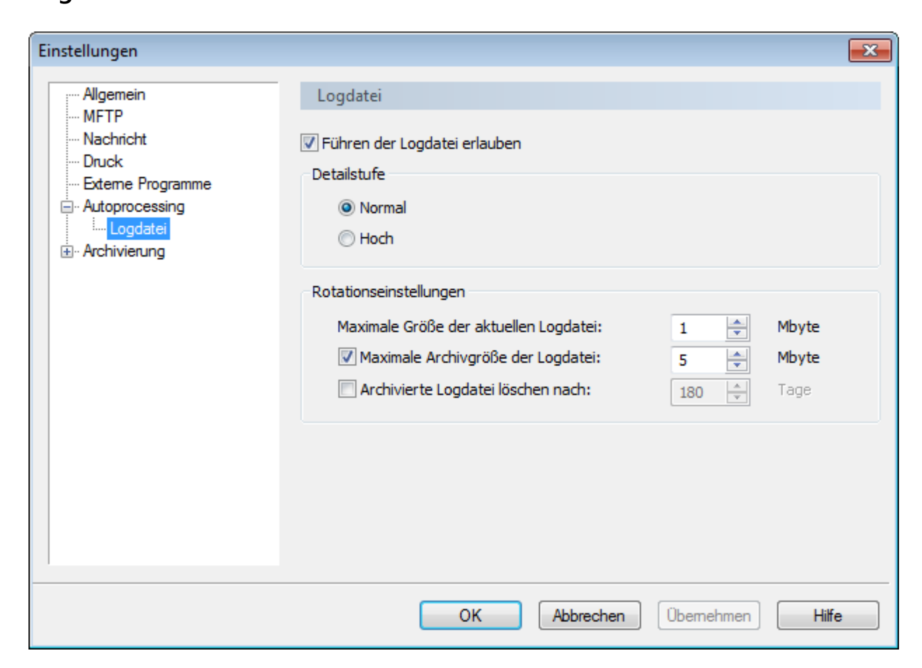


Abbildung 32. Autoprocessing-Logdatei einstellen

3 Deaktivieren Sie das Kontrollkästchen **Logdatei führen** (standardmäßig aktiviert), um das Führen einer Autoprocessing–Logdatei zu unterbinden.

Wenn dieses Kontrollkästchen deaktiviert ist, ist das Einstellen weiterer Parameter für die Autoprocessing–Logdatei nicht möglich.

4 Wählen Sie einen der folgenden Punkte in Gruppe **Detailstufe**:

- **Normal** (standardmäßig ausgewählt): nur die wichtigste Information wird geloggt.
- **Hoch**: jede Art von Information wird geloggt.

5 Geben Sie für die Gruppe **Rotationseinstellungen** folgende Parameter an:

- Geben Sie im Feld **Maximale Größe der aktuellen Logdatei** die Größe der Logdatei in Megabytes an (standardmäßig 1).

  Wenn die Größe der laufenden Logdatei diese Größe übersteigt, erhält diese Datei den Archivstatus, und es wird eine neue aktuelle Logdatei erzeugt.

- Aktivieren Sie das Kontrollkästchen **Maximale Archivgröße der Logdatei**, um die maximale Größe der Datei zu bestimmen. Geben Sie im Feld rechts davon die Größe in Megabytes ein (standardmäßig 5).

  Wenn die Gesamtgröße der archivierten Logdateien diesen Wert übersteigt, werden die ältesten Archivdateien sukzessiv gelöscht, bis die Gesamtgröße der Archivdateien den angegebenen Wert erreicht oder darunter fällt.

- Aktivieren Sie das Kontrollkästchen **Archivierte Logdatei löschen nach**, um die Aufbewahrungszeit der Archivdateien einzuschränken. Geben Sie im Feld rechts davon die maximale Dauer der Speicherung von Archivdateien in Tagen ein (standardmäßig 180).

  Wenn die Dauer der Archivierung (Differenz zwischen der aktuellen Zeit und dem Zeitpunkt der Überführung der Datei in ein Archiv) den angegebenen Wert übersteigt, wird die entsprechende Archivdatei gelöscht.



Hinweis. Wenn das Kontrollkästchen **Maximales Logdateialter** aktiviert ist, ist es nicht empfehlenswert, die Systemzeit umzustellen, da dies negative Folgen nach sich ziehen kann.

6. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern.

6

Einstellungen

Allgemeine Parameter einstellen

Führen Sie folgende Schritte aus, um allgemeine Parameter in „Business Mail“ einzustellen:

1 Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Allgemein**.

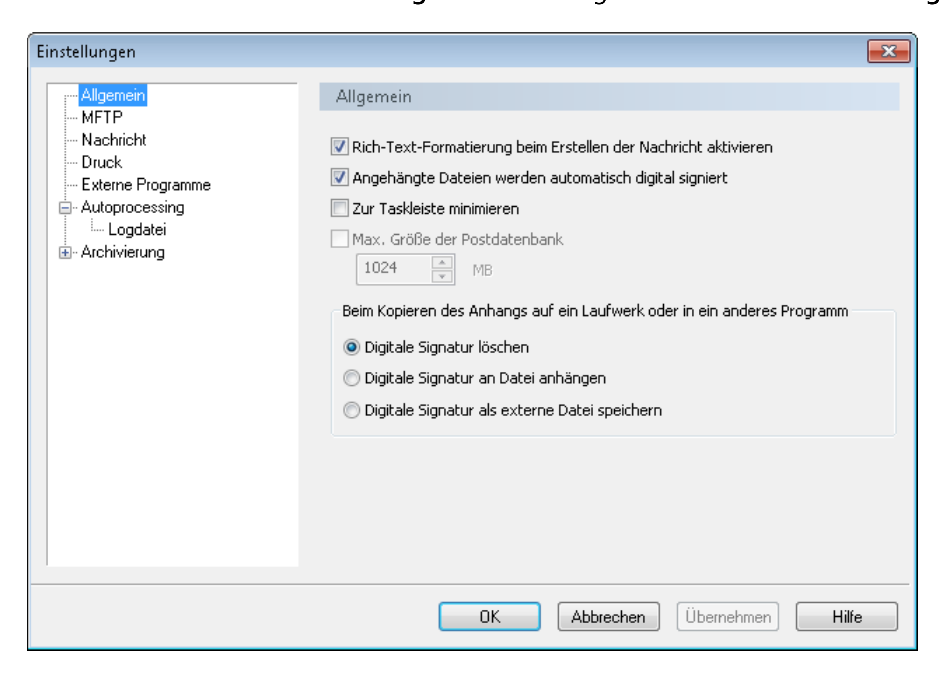


Abbildung 33. Allgemeine Einstellungen in ViPNet Business Mail

3 Wollen Sie beim Erstellen von Nachrichten die Möglichkeiten der Textformatierung verwenden, aktivieren Sie das Kontrollkästchen **Rich-Text-Formatierung beim Erstellen der Nachricht aktivieren** (standardmäßig deaktiviert). Dabei wird die Formatierungsleiste im Fenster zum Verfassen von Nachrichten (s. Fenster zum Anzeigen und Verfassen von Nachrichten auf S. 40) angezeigt.

Wir empfehlen Nachrichten ohne Formatierung zu versenden, wenn die Nachrichtenempfänger eine frühere Version von ViPNet Business Mail verwenden, in der Formatierung nicht unterstützt wird. Wird eine Nachricht mit Formatierung an einen solchen Empfänger gesendet, erhält dieser Empfänger den Text Ihrer Nachricht als Anhang `BODY-<Registrierungsnummer der Nachricht>.rtf` und kann ihn mit Hilfe des Textverarbeitungsprogramms lesen, z.B. Microsoft Office Word oder Microsoft WordPad.

4 Aktivieren Sie das Kontrollkästchen **Zur Taskleiste minimieren** (standardmäßig deaktiviert), um das Programmfenster beim Klicken auf die Schaltfläche **Schließen** in den Infobereich der Taskleiste zu minimieren.

5 Deaktivieren Sie das Kontrollkästchen **Angehängte Dateien werden automatisch digital signiert** (standardmäßig aktiviert), um beim Signieren einzelner Dateien die digitalen Signaturen abzutrennen (s. Datei digital signieren auf S. 74).

6 Aktivieren Sie das Kontrollkästchen **Max. Größe der Postdatenbank**, um die Größe der Nachrichtendatenbank einzuschränken. Geben Sie im Feld darunter die Größe in MB an.

Wenn die Größe der Postdatenbank begrenzt wird, unterbricht das Programm beim Erreichen der angegebenen Maximalgröße das Abholen von Nachrichtenpaketen aus dem Ordner des MFTP–Moduls (d. h. Sie werden keine neuen Nachrichten mehr empfangen).

7 Wählen Sie in der Gruppe **Beim Kopieren des Anhangs auf dem Laufwerk oder in ein anderes Programm** eine der folgenden Aktionen aus:

- o **Digitale Signatur löschen** (standardmäßig aktiviert);
- o **Digitale Signatur an Datei anhängen**;
- o **Digitale Signatur als externe Datei speichern**.

Weitere Informationen über angehängte Signaturen und Signaturen in externen Dateien finden Sie in Dateisignatur anhängen und abtrennen (auf S. 75).

8 Nachdem Sie alle notwendigen Einstellungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Archivierung einstellen

Allgemeine Archivierungsparameter

Bei der Konfiguration der manuellen oder automatischen Archivierung von Nachrichten (s. Nachrichten archivieren auf S. 60) können Sie festlegen, welche Nachrichten in das Archiv verschoben und wie die Nachrichtenanhänge im Archiv gespeichert werden sollen.

Führen Sie die folgenden Schritte aus, um die Archivierungseinstellungen zu konfigurieren:

1 Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** den Bereich **Archivierung**.

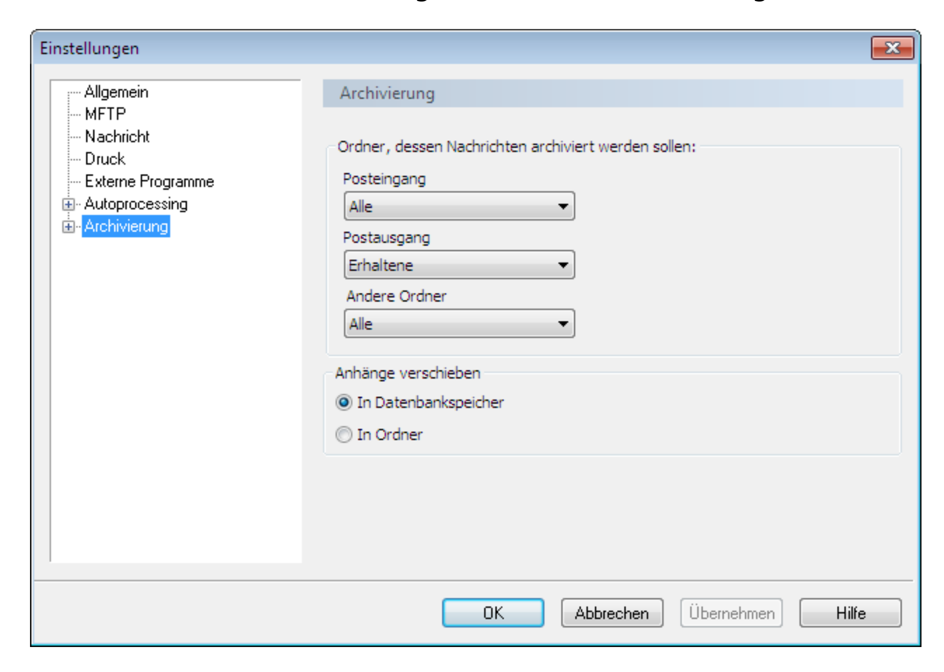


Abbildung 34. Archivierungsparameter einstellen

3 Wählen Sie in Gruppe **Ordner, dessen Nachrichten archiviert werden sollen** die Kategorien von Nachrichten aus, die archiviert werden sollen:

- Wählen Sie in der Dropdownliste **Posteingang** entweder den Eintrag **Gelesene** oder **Alle** (standardmäßig ausgewählt) aus, um zu bestimmen, welche eingegangenen Nachrichten archiviert werden sollen.
- Wählen Sie in der Dropdownliste **Postausgang** den Eintrag **Gesendete**, **Erhaltene**, **Gelesene** oder **Alle** (standardmäßig ausgewählt) aus, um zu bestimmen, welche ausgehenden Nachrichten archiviert werden sollen.
- Wählen Sie in der Dropdownliste **Anderes** den Eintrag **Keine** oder **Alle** (standardmäßig ausgewählt) aus, um zu bestimmen, welche eingegangenen Nachrichten aus den Ordnern **Gelöschte Objekte** und **Audit** archiviert werden sollen.

Wenn für alle Ordner der Wert **Alle** ausgewählt wird (vollständige Archivierung), dann wird bei der Archivierung die aktuelle Postdatenbank in ein Archiv umgewandelt. Für die Weiterarbeit wird eine neue Postdatenbank erstellt. Bei unvollständiger Archivierung wird ein neues Archiv erstellt. In dieses Archiv werden die zu archivierenden Nachrichten kopiert. Demgemäß nimmt die vollständige Archivierung deutlich weniger Zeit in Anspruch als die unvollständige.



Achtung! Wenn mit Hilfe von ViPNet Business Mail täglich eine hohe Anzahl an Nachrichten verarbeitet wird, dann ist es empfehlenswert, für alle Nachrichten in allen Ordnern die vollständige Archivierung einzustellen.

4 Geben Sie in Gruppe **Anhänge verschieben** mit Hilfe des Optionsfeldes die Art der Speicherung der Anhängen:

- **In Datenbankspeicher**: Anhänge werden zur Datenbank hinzugefügt und im Archiv (standardmäßig) gemeinsam mit den Nachrichten gespeichert. Bei dieser Speicherungsart enthält das Archiv nur eine Datenbankdatei, die ggf. einfach auf einen externen Datenträger kopiert oder verschoben werden kann.
- **In Ordner**: Anhänge werden in Ordnern getrennt von den Nachrichten gespeichert. In diesem Fall enthält das Archiv eine Datei mit der Nachrichtendatenbank und eine Reihe von Ordnern mit Anhängen.



Achtung! Die Speicherungsart der Anhänge wird nur bei unvollständiger Archivierung berücksichtigt.

5 Nachdem Sie alle notwendigen Einstellungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Parameter der automatischen Archivierung einstellen

Führen Sie folgende Schritte aus, um die Parameter der automatischen Archivierung einzustellen:

1 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Eintrag **Archivierung** > **Automatische Archivierung**.

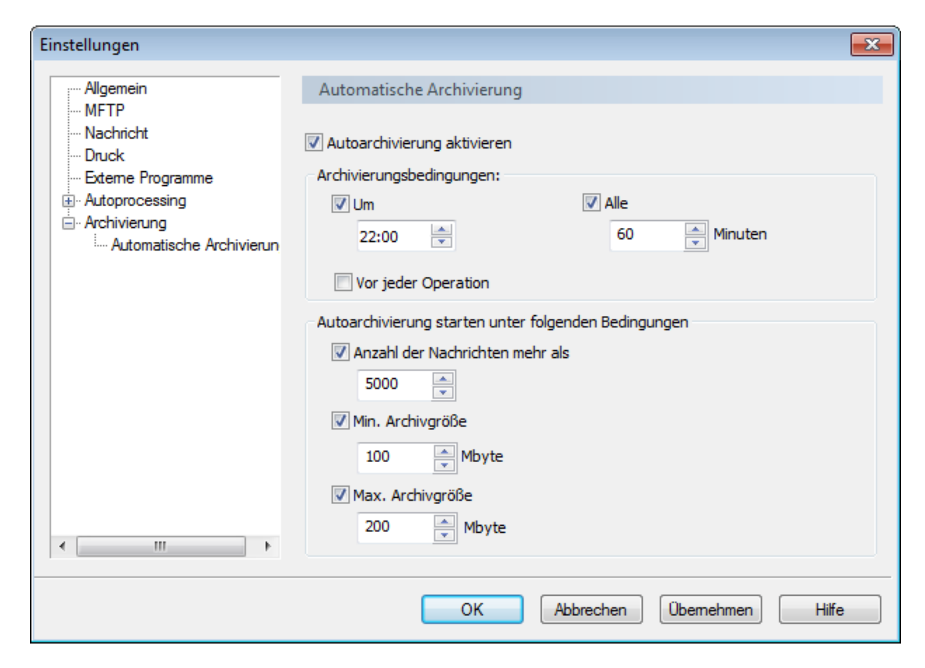


Abbildung 35. Parameter für die automatische Archivierung

2 Aktivieren Sie das Kontrollkästchen **Autoarchivierung aktivieren** (standardmäßig deaktiviert), um die automatische Archivierung einzuschalten.

3 Wenn die automatische Archivierung eingeschaltet ist, dann aktivieren Sie in Gruppe **Archivierungsbedingungen** eines oder mehrere Kontrollkästchen:

- Aktivieren Sie das Kontrollkästchen **Um**, falls die Bedingungen zu einer bestimmten Zeit geprüft werden sollen. Geben Sie im Feld unter dem Kontrollkästchen die Prüfzeit ein (standardmäßig ist das Kontrollkästchen aktiviert, für die Zeit ist 22:00 angegeben).
- Aktivieren Sie das Kontrollkästchen **Alle**, falls die Bedingungen in bestimmten Zeitabständen geprüft werden sollen. Geben Sie im Feld unter dem Kontrollkästchen die Zeit in Minuten an (standardmäßig ist das Kontrollkästchen aktiviert, für die Zeit sind 60 Minuten angegeben).
- Aktivieren Sie das Kontrollkästchen **Vor jeder Operation** (standardmäßig deaktiviert), um die Archivierungsbedingungen vor jedem Senden und Empfangen von Nachrichten zu prüfen.



Hinweis. Wenn in Gruppe **Archivierungsbedingungen** mehrere Kontrollkästchen aktiviert sind, wird die Prüfung der Archivierungsbedingungen in allen angegebenen Fällen durchgeführt.

---

4 Wenn die automatische Archivierung eingeschaltet ist, dann aktivieren Sie in Gruppe **Autoarchivierung starten unter folgenden Bedingungen** eines oder mehrere Kontrollkästchen:

- Aktivieren Sie das Kontrollkästchen **Anzahl der Nachrichten mehr als**, um die Autoarchivierung bei Ansammlung einer bestimmten Nachrichtenmenge zu starten. Geben Sie im Feld darunter die Anzahl der Nachrichten an (standardmäßig 5000).
- Aktivieren Sie das Kontrollkästchen **Min. Archivgröße**, um die Autoarchivierung beim Erreichen einer bestimmten Archivgröße zu starten. Geben Sie im Feld darunter die Größe in Megabytes an (standardmäßig 100).



Hinweis. Wenn beide Kontrollkästchen **Anzahl der Nachrichten mehr als** und **Min. Archivgröße** aktiviert sind, dann erfolgt die Archivierung bei Erfüllung zumindest einer der angegebenen Bedingungen.

- Aktivieren Sie das Kontrollkästchen **Max. Archivgröße**, um die maximale Archivgröße anzugeben. Geben Sie im Feld darunter die Größe in Megabytes an (standardmäßig 200).

  Wenn die Gesamtgröße der zu archivierenden Nachrichten die angegebene maximale Archivgröße übersteigt, werden mehrere Nachrichtenarchive erstellt. Die Größe jedes einzelnen Archivs wird kleiner als der angegebene Wert sein.

5 Nachdem Sie alle notwendigen Einstellungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Nachrichtenparameter einstellen

Führen Sie folgende Schritte aus, um die Parameter für die Arbeit mit Nachrichten einzustellen:

1 Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Nachricht**.

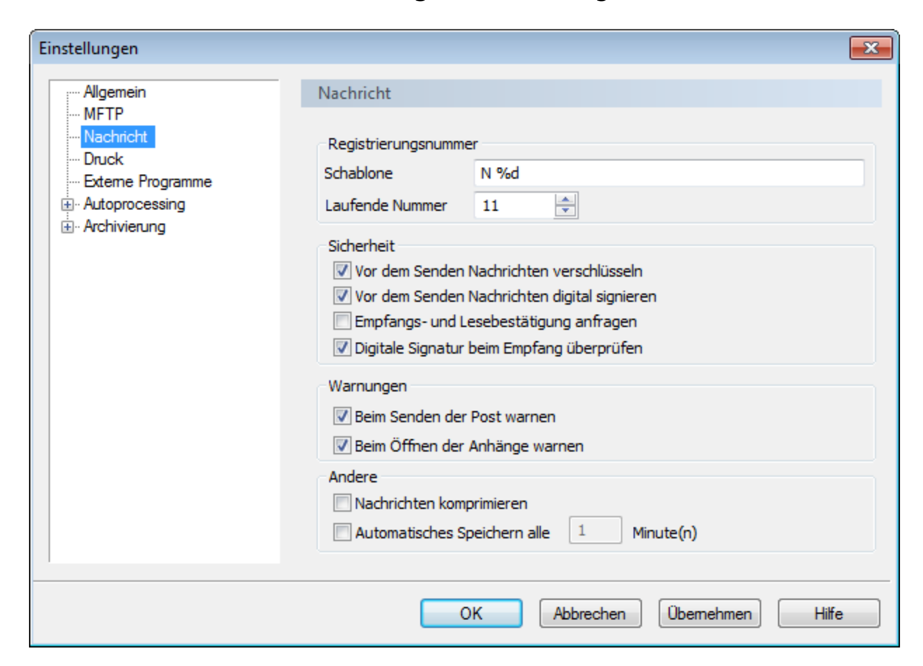


Abbildung 36. Nachrichtenparameter

3 Stellen Sie bei Notwendigkeit das Format der Registrierungsnummer ein.

Eine Registrierungsnummer bekommt jede Nachricht bei ihrer Neuerstellung zugewiesen. Eingehende Nachrichten besitzen Registrierungsnummern, die vom Absender zugewiesen wurden. Registrierungsnummern werden in der Nachrichtenliste eingeblendet (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31).

Führen Sie innerhalb der Gruppe **Registrierungsnummer** folgende Schritte aus, um das Format der Registrierungsnummer zu ändern:

- Geben Sie im Feld **Schablone** die Maske für den permanenten Teil der Nummer an. Der permanente Teil kann nicht mehr als 12 Zeichen beinhalten und muss unbedingt die Zeichenfolge „%d“ enthalten, die später durch die laufende Nummer ersetzt wird.
- Falls die laufende Nummer geändert werden soll, geben Sie im Feld **Laufende Nummer** eine Zahl an, die größer als die zu diesem Zeitpunkt eingetragene Nummer, aber nicht größer als 999999999 ist.

4 Führen Sie in der Gruppe **Sicherheit** folgende Schritte aus, um die Parameter für Verschlüsselung und digitale Signatur einzustellen:

- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vor dem Senden Nachrichten verschlüsseln**.

- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vor dem Senden Nachrichten digital signieren**. Wenn dieses Kontrollkästchen aktiviert ist, werden der Nachrichtentext und alle Anhänge automatisch mit dem aktuellen Zertifikat signiert (s. Digitale Signatur in „Business Mail" auf S. 66).
- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Empfangs– oder Lesebestätigung anfragen** (s. Anfrage der Empfangs– und Lesebestätigungen als separate Nachricht auf S. 44).
- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Digitale Signatur beim Empfang überprüfen**.

5 Führen Sie in der Gruppe **Warnungen** folgende Aktionen aus, um die Parameter für Benachrichtigungen beim Anzeigen der Anhänge und Versenden der Nachrichten einzustellen:

- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Beim Öffnen der Anhänge warnen**.

  Wenn dieses Kontrollkästchen aktiviert ist, wird vom Programm vor dem Anzeigen eines Anhangs eine Warnmeldung angezeigt.
- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Beim Senden der Post warnen**.

  Wenn dieses Kontrollkästchen aktiviert ist, bittet das Programm vor dem Versenden einer Nachricht um Betätigung.

6 In Gruppe **Andere** sind folgende Einstellungen möglich:

- Aktivieren Sie das Kontrollkästchen **Nachrichten komprimieren** (standardmäßig deaktiviert), um die Nachrichten im komprimierten Zustand zu versenden. Vor dem Versand werden die Nachrichten durch einen Komprimierungsalgorithmus verarbeitet.
- Aktivieren Sie das Kontrollkästchen **Automatisches Speichern alle ... Minute(n)** (standardmäßig deaktiviert), um eine automatische Zwischenspeicherung der bearbeiteten Nachrichten zu ermöglichen. Geben Sie im Feld rechts davon einen Zeitabstand für die automatische Speicherung in Minuten an.

MFTP–Modul einstellen

Führen Sie folgende Schritte aus, um die Parameter für das MFTP–Modul einzustellen:

1 Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **MFTP**.

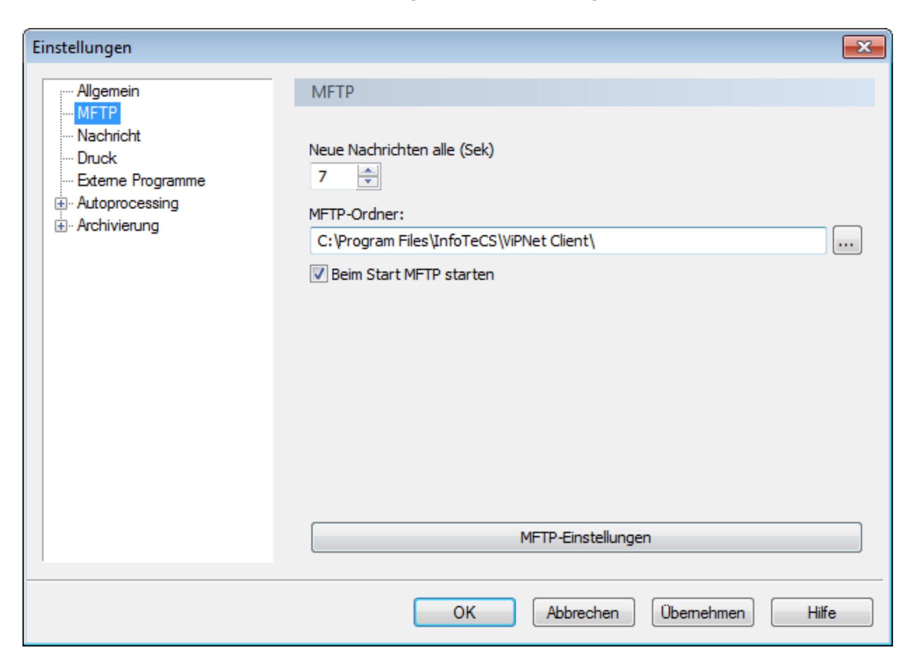


Abbildung 37. Einstellungen des MFTP–Moduls

3 Im Abschnitt **MFTP** können, wenn nötig, folgende Parameter geändert werden:

- Geben Sie im Feld **Neue Nachrichten alle (Sek)** den benötigten Zeitabstand für das Abrufen der Nachrichten in Sekunden an.
- Wenn Sie den MFTP–Ordner ändern wollen, klicken Sie auf die Schaltfläche ... und geben Sie im Fenster **Ordner auswählen** den Ordner an, in dem sich das MFTP–Modul befindet.



Achtung! Der Ordner des MFTP–Moduls sollte im Normalfall nicht geändert werden.

- Deaktivieren Sie das Kontrollkästchen **Beim Start MFTP starten** (standardmäßig aktiviert), falls das MFTP–Modul beim Start von „Business Mail“ nicht gestartet werden soll.

4 Klicken Sie auf die Schaltfläche **MFTP Einstellungen**, um das Fenster mit Einstellungen aufzurufen, das im Hauptfenster des MFTP–Moduls zur Verfügung gestellt wird.

Weitere Informationen über das MFTP–Modul und seine Einstellungen sind im Handbuch „ViPNet MFTP. Administratorhandbuch“ enthalten.

5 Nachdem Sie alle notwendigen Einstellungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Druckparameter einstellen

Führen Sie folgende Schritte aus, um die Parameter für den Druck von Nachrichten einzustellen:

1 Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Druck**.

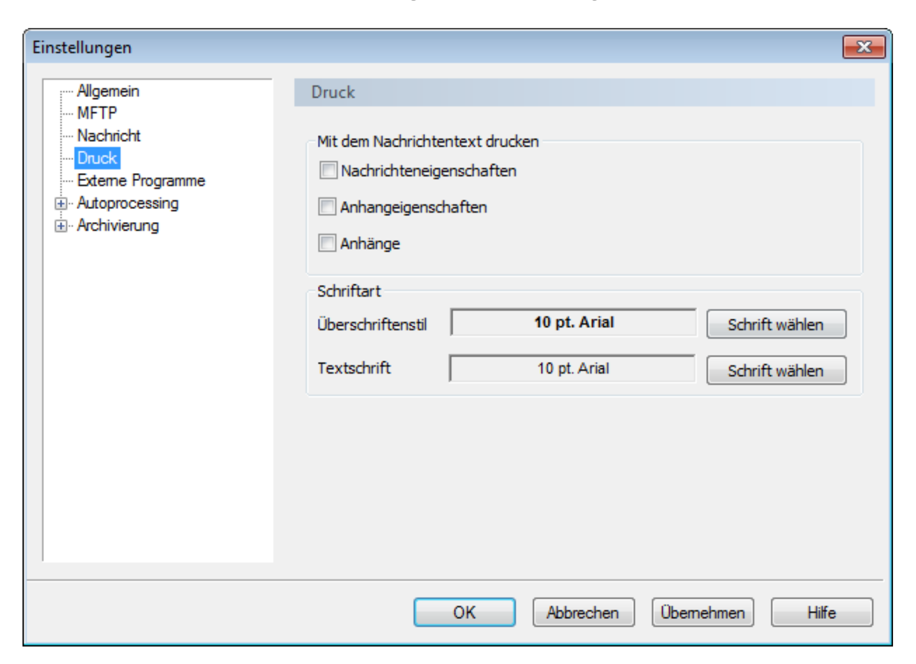


Abbildung 38. Druckeinstellungen

3 Geben Sie in der Gruppe **Mit dem Nachrichtentext drucken** die Zusatzinformationen an, die dem Nachrichtentext hinzugefügt werden sollen, indem Sie die notwendigen Kontrollkästchen aktivieren (standardmäßig sind alle Kontrollkästchen deaktiviert):

- **Nachrichteneigenschaften.**
- **Anhangeigenschaften.**
- **Anhänge.**

4 Um die Schriftart der Überschriften und des Textes beim Drucken von Nachrichten, die ohne Formatierung erstellt wurden, und die Schriftart der oben genannten zusätzlichen Informationen zu ändern, klicken Sie auf die Schaltfläche **Schrift wählen** rechts vom Feld **Überschriftenstil** oder **Textschrift** und geben im Fenster **Schriftart wählen** die Parameter für die Schrift an.

5 Nachdem Sie alle notwendigen Einstellungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Externe Programme einstellen

In ViPNet Business Mail gibt es die Möglichkeit, externe Programme aufrufen. Zum Starten eines externen Programms, wählen Sie im „Business Mail" Hauptfenster im Menü **Extras** den Punkt **Externes Programm aufrufen**.

Führen Sie folgende Schritte aus, um die Liste der verfügbaren externen Programme zu modifizieren:

1 Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Externe Programme**.

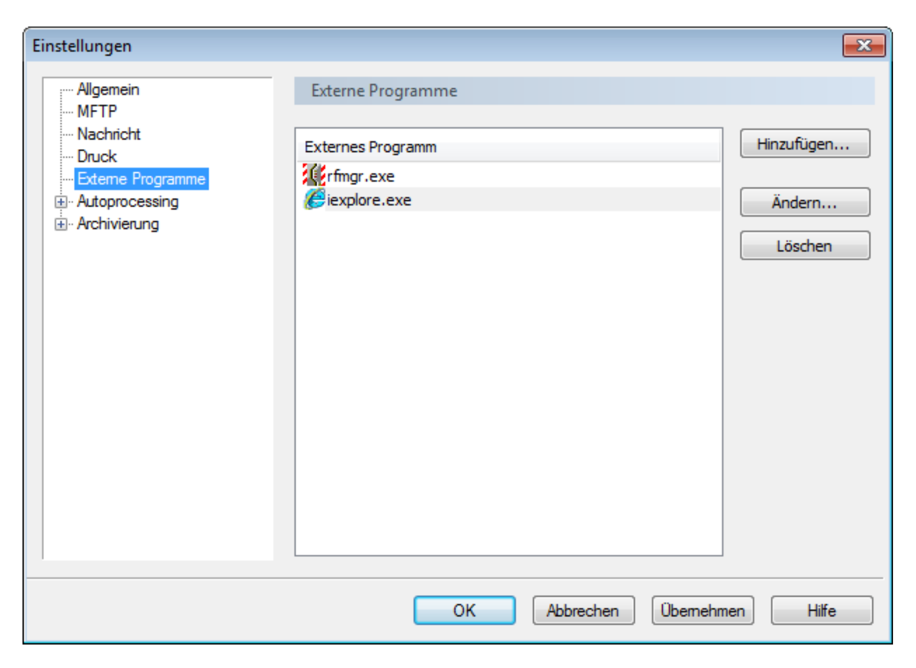


Abbildung 39. Externe Programme einstellen

3 So fügen Sie eine Anwendung in die Liste der Programme hinzu, die für den Aufruf aus „Business Mail" verfügbar sind:

- Klicken Sie auf die Schaltfläche **Hinzufügen**.
- Geben Sie im Fenster **Externes Programm** den Pfad zur ausführbaren Datei der externen Anwendung an und klicken dann auf **Weiter**.
- Geben Sie im Fenster **Name des externen Programms** die Programmbezeichnung an, die auf der „Business Mail Benutzeroberfläche eingeblendet wird, und klicken Sie dann auf **Fertig**.

4 Wählen Sie das Programm in der Liste aus und klicken auf **Ändern**, um den Pfad oder den Namen der externen Anwendung zu ändern.

5 Um ein Programm aus der Liste zu entfernen, wählen Sie es aus und klicken auf **Löschen**.

6 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Arbeiten mit Administratorrechten

Das Programm ViPNet Business Mail sieht die Möglichkeit vor, mit Administratorrechten zu arbeiten. Beim Arbeiten im Administrator–Modus werden folgende Funktionen und Einstellungen verfügbar sein:

- Zusätzliche Möglichkeiten und Parameter des Programms (auf S. 114).
- Zusätzliche Sicherheitseinstellungen (auf S. 115).
- Benutzer–Authentisierungsmodus ändern (auf S. 116).

Beim Arbeiten im Administrator–Modus fallen alle durch die Benutzerrechte (auf S. 177) festgelegten Einschränkungen weg.

So melden Sie sich am Programm als Administrator an:

1. Wählen Sie im ViPNet Business Mail Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** den Eintrag **Sicherheitseinstellungen**.
2. Klicken Sie im Fenster **Sicherheitseinstellungen** auf die Registerkarte **Administrator**, und klicken Sie dann auf die Schaltfläche **Administrator–Login**.
3. Geben Sie im Fenster **Administrator-Anmeldung** das Passwort des ViPNet Netzwerkknoten–Administrators ein (s. Netzwerkknoten Administrator auf S. 178).

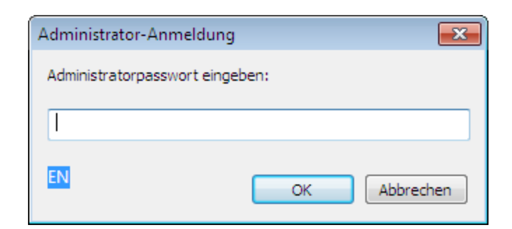


Abbildung 40. Passwort des Netzwerkknoten–Administrators eingeben

4. Klicken Sie auf **OK**. Wenn das eingegebene Passwort gültig ist, wird das Programm neu gestartet, und zusätzliche Einstellungen werden zur Verfügung gestellt.

Zusätzliche Möglichkeiten und Parameter des Programms

Beim Arbeiten im Administrator–Modus ist es möglich, Einträge über gelöschte Nachrichten aus dem Ordner **Audit** zu entfernen. In allen Ordnern von „Business Mail“ ist im Kontextmenü der Nachricht der Befehl **Vollständiges Löschen** verfügbar. Beim vollständigen Löschen wird die Nachricht aus der Postdatenbank entfernt, ohne dass darüber ein Eintrag im Ordner **Audit** erzeugt wird.

Wenn die Benutzerrechte (auf S. 177) von „Business Mail“ Einschränkungen unterliegen, fallen im Administrator–Modus alle Einschränkungen weg.

Im Administrator–Modus wird außerdem im Fenster **Einstellungen** der Bereich **Administrator** verfügbar, in dem das Abspeichern von Informationen über gelöschte Nachrichten im Ordner **Audit** deaktiviert werden kann:

1 Melden Sie sich in „Business Mail" als Administrator an (s. Arbeiten mit Administratorrechten auf S. 114).

2 Klicken Sie im Programmfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 31) im Menü **Extras** auf den Eintrag **Einstellungen**.

3 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Eintrag **Administrator**.

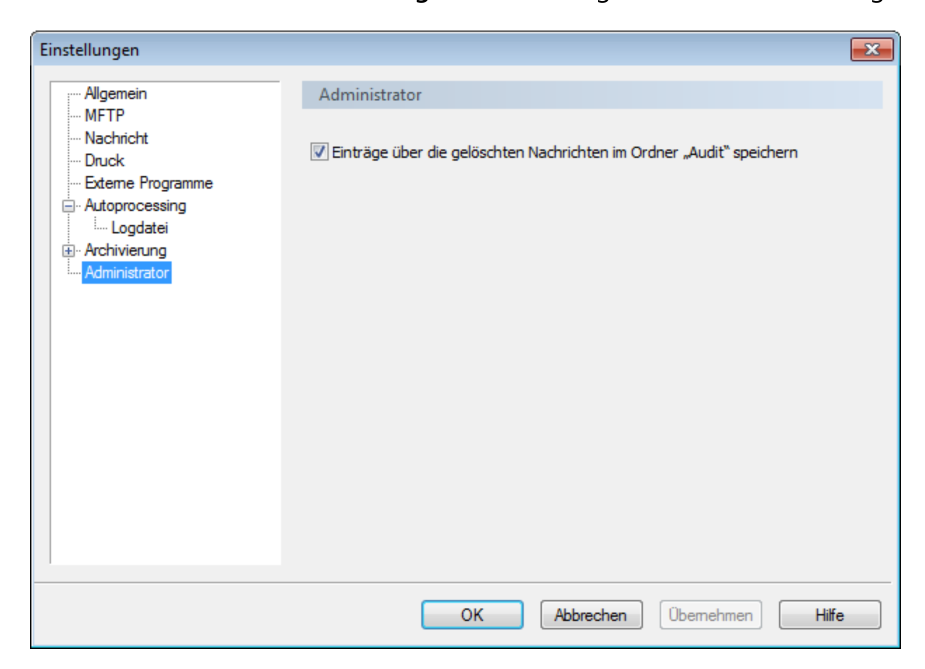


Abbildung 41. Zusätzliche Einstellungen im Bereich „Administrator"

4 Deaktivieren Sie das Kontrollkästchen **Einträge über die gelöschten Nachrichten im Ordner „Audit" speichern** (standardmäßig aktiviert), um das Abspeichern von Informationen über gelöschte Nachrichten im Ordner **Audit** zu deaktivieren.

5 Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Zusätzliche Sicherheitseinstellungen

Neben den erweiterten Einstellungen im Bereich **Administrator** sind im Administratormodus zusätzlich die folgenden Einstellungen in der Registerkarte **Administrator** im Fenster **Sicherheitseinstellungen** konfigurierbar:

- **Passwort darf in der Registry gespeichert werden**: erlaubt es dem Benutzer des Netzwerkknotens, das Kontrollkästchen **Passwort speichern** bei der Anmeldung im Programm ViPNet Business Mail zu aktivieren. Wenn das Kontrollkästchen **Passwort speichern** aktiviert ist, wird das Benutzerpasswort in der Windows-Registry gespeichert und automatisch in das Passwortfeld beim Start von ViPNet Monitor eingefügt.

Hinweis. Dieser Parameter wird durch den ViPNet Netzwerkadministrator im Programm ViPNet Network Manager oder ViPNet Administrator festgelegt und mit der Schlüsseldistribution oder mit der Aktualisierung der Adresslisten und Schlüssel auf den Knoten übermittelt. Der Netzwerkknotenadministrator kann das Kontrollkästchen **Passwort darf in der Registry gespeichert werden** aktivieren oder deaktivieren, diese Änderung wird bis zur nächsten Aktualisierung der Adresslisten und Schlüssel gelten. Nach der nächsten Aktualisierung wird das Kontrollkästchen den durch den ViPNet Administrator definierten Einstellungen entsprechen.

- **Automatisch in ViPNet anmelden**: ermöglicht die Anmeldung im Programm ViPNet Business Mail ohne vorhergehende Eingabe des ViPNet-Benutzerpassworts im Anmeldefenster des Programms. Wenn das Kontrollkästchen aktiviert ist, wird das Anmeldefenster beim Start des Programms auf dem aktuellen Netzwerkknoten nicht eingeblendet. Die Anmeldung in ViPNet Monitor erfolgt automatisch. Dies ist in den folgenden Fällen möglich:
  - bei Verwendung des Authentisierungsmodus **Nur das Passwort**: wenn das Passwort in der Registry gespeichert wird (d. h., das Kontrollkästchen **Passwort darf in der Registry gespeichert werden** ist aktiviert) und im Anmeldefenster des Programms das richtige Passwort angegeben und das Kontrollkästchen **Passwort speichern** aktiviert ist;
  - bei Verwendung des Authentisierungsmodus **Passwort auf Authentisierungsgerät** sowie **PIN und Authentisierungsgerät**: wenn das externe Gerät an den Computer angeschlossen ist und im Anmeldefenster des Programms die korrekte PIN angegeben und das Kontrollkästchen **PIN speichern** aktiviert ist.
- **Zertifikate aus dem Zertifikatsspeicher des Betriebssystems erlauben**: diese Einstellung ermöglicht neben der Verwendung der Zertifikate aus dem eigenen Zertifikatspeicher (Programmspeicher) auch die Verwendung der Zertifikate aus dem Zertifikatspeicher des Betriebsystems. Dies kann dann erforderlich sein, wenn in ViPNet Software der Cryptoprovider eines Drittherstellers (zum Beispiel CryptoPro) oder von externen Zertifizierungsstellen (außerhalb des ViPNet Netzwerks) herausgegebene Zertifikate verwendet werden sollen.
- **Nur eigenen Zertifikatlisten vertrauen**: wenn dieses Kontrollkästchen deaktiviert ist, wird die Suche nach dem Stammzertifikat bei der Zertifikatüberprüfung nicht nur im internen Zertifikatspeicher der ViPNet Software, sondern auch im Systemspeicher **Vertrauenswürdige Stammzertifizierungsstellen** und **Zwischenzertifizierungsstellen** durchgeführt.
- **Ignorieren, wenn die Zertifikatsperrlisten nicht vorhanden sind**: dieses Kontrollkästchen sollte dann aktiviert werden, wenn im System Zertifikate verwendet werden, die von einer externen Zertifizierungsstelle veröffentlicht wurden, da Informationen über Zertifikatsperrlisten in solchen Zertifikaten fehlen können.

Benutzer–Authentisierungsmodus ändern

Der Authentisierungsmodus bestimmt, welche Daten ein Benutzer beim Login ins Programm ViPNet Business Mail anzugeben hat. Um den Authentisierungsmodus zu ändern, gehen Sie wie folgt vor:

1 Melden Sie sich im Programm im Administratormodus an.

2 Klicken Sie auf die Schaltfläche **Ändern** in der Registerkarte **Schlüssel** im Fenster **Sicherheitseinstellungen**.

3 Wählen Sie einen der Modi im Fenster **Authentisierungsmodus** aus. Die Beschreibung möglicher Authentisierungsmodi sehen Sie im Abschnitt Authentisierungsmodi (auf S. 26).



Hinweis. Der Modus **Passwort auf Authentisierungsgerät** kann nicht ausgewählt werden, da er den aktuellen Sicherheitsanforderungen nicht mehr entspricht.

Falls die Authentifizierung mit Hilfe eines Zertifikats durchgeführt wird, schließen Sie dann das externe Gerät an und wählen Sie anschließend das benötigte Zertifikat in der Liste der auf dem Gerät festgestellten Zertifikate aus. Falls bei der Auswahl des Zertifikats Schwierigkeiten auftreten, folgen Sie den Anweisungen im Abschnitt Authentifizierung mittels Zertifikat kann nicht durchgeführt werden (auf S. 165).

Falls die Authentifizierung mit Hilfe eines privaten Schlüssels durchgeführt wird, schließen Sie dann das externe Gerät an, um um den privaten Schlüssel des ViPNet Benutzers auf dem Gerät zu speichern. Beim Speichern des privaten Benutzerschlüssels (Schutzschlüssels) auf einem externen Gerät sollte eine Besonderheit beachtet werden: wenn der Benutzer die Funktionen der Signatur und Verschlüsselung innerhalb von Anwendungen anderer Hersteller (zum Beispiel Microsoft ViPNet VPN) verwendet, dann wird es nachdrücklich empfohlen, den entsprechenden Schlüsselcontainer ebenfalls auf diesem Gerät zu speichern. Anderenfalls wird das Signieren und Verschlüsseln in Drittanwendungen nicht möglich sein, da es Probleme mit dem Zugang zum Schutzschlüssel geben wird. Der Schlüsselcontainer kann aus dem laufenden Ordner in einen anderen Ordner auf dem Laufwerk verschoben werden. In diesem Fall werden Sie jedoch jedes Mal beim Signieren und Verschlüsseln in einer Drittanwendung zur Passworteingabe aufgefordert.



Achtung! Wenn bei Verwendung des Authentisierungsmodus **PIN und Authentisierungsgerät** das externe Gerät getrennt wird, dann wird der Computer automatisch gesperrt – in Übereinstimmung mit den Einstellungen, die im Administratormodus konfiguriert wurden. Zum Fortsetzen der Arbeit sollte das betroffene Gerät wieder an den Computer angeschlossen werden. Wenn nötig, können die Parameter der automatischen Sperre des Computers und des IP-Traffics auch geändert werden.

4 Klicken Sie auf **OK**.

In der Registerkarte **Schlüssel** in der Gruppe **Authentifizierung** werden die Werte in den Feldern **Authentisierungsmodus** und **Authentisierungsgerät** entsprechend dem gewählten Modus geändert.

Bei Netzwerken auf Basis der Software ViPNet Administrator kann der Authentisierungsmodus vom Netzwerkadministrator auch im Programm ViPNet Key and Certification Authority geändert werden. Wenn für einen Benutzer vom Administrator der Authentisierungsmodus mittels Zertifikat ausgewählt wurde, dann sollte der betroffene Benutzer das externe Authentisierungsgerät mitsamt dem Zertifikat sowie seinem privaten Schlüssel dem Administrator für die Registrierung zur Verfügung stellen. Dabei sollten alle Anforderungen erfüllt sein, die im Hinweis im Abschnitt PIN und Authentisierungsgerät

(auf S. 29) aufgezählt wurden. Nachdem dem Benutzer ein neuer Authentisierungsmodus zugewiesen wurde, wird vom Administrator ein Update der Netzwerkknotenschlüssel versendet. Nach Annahme dieses Schlüsselupdates kann sich der Benutzer nur mehr im zugewiesenen Authentisierungsmodus auf dem Netzwerkknoten anmelden.



7 Sicherheitseinstellungen

Ändern des Benutzerpassworts

Es wird empfohlen, das Benutzerpasswort alle 3 Monate zu wechseln. Die Häufigkeit von Passwortänderungen wird allgemein von der Sicherheitsrichtlinie des Unternehmens bestimmt.

Das aktuelle Benutzerpasswort sollte in folgenden Fällen geändert werden:

- Nach Ablauf der Gültigkeitsdauer des aktuellen Passwortes (wenn die Gültigkeitsdauer begrenzt ist).
- Beim Erhalten von Updates aus dem Programm ViPNet Key and Certification Authority, die ein neues Benutzerpasswort erhalten, die ein neues Benutzerpasswort enthalten. In diesem Fall wird ein Dialogfeld mit der Meldung „Benutzerpasswort-Änderung wird empfohlen" angezeigt. Das Passwort wird dabei jedoch nicht automatisch gewechselt und sollte daher manuell geändert werden.
- Wenn der Schlüsselcontainer nicht durch ein Passwort, sondern mit dem privaten Schlüssel des ViPNet Benutzers geschützt wird, dann stimmt das Schlüsselcontainer-Passwort mit dem Benutzerpasswort überein. Deswegen sollte bei einem Wechsel des Schlüsselcontainer Passworts (s. Schlüsselcontainerpasswort ändern auf S. 159) auch das Benutzerpasswort geändert werden.

Außerdem wird es empfohlen, das Benutzerpasswort nach dem Durchführen der primären Initialisierung bei der ersten Anmeldung in einem ViPNet Programm ViPNet zu wechseln. Dies erhöht die Sicherheit des Passworts, da es dem Administrator nicht mehr bekannt sein wird.

Zum Ändern des Benutzerpassworts:

1 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Passwort**.

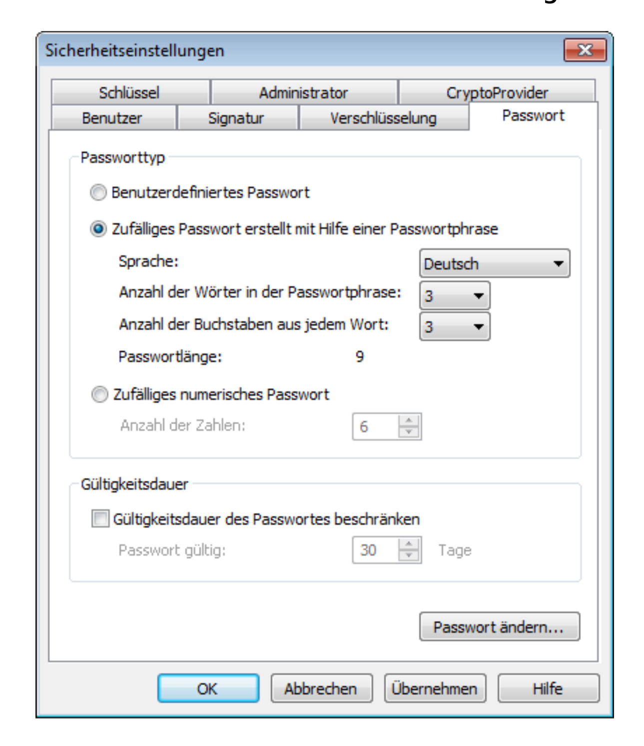


Abbildung 42. Aktuelles Benutzerpasswort ändern

2 Wählen Sie im Bereich **Passworttyp** den passenden Typ, für das neue Passwort aus:

- **Benutzerdefiniertes Passwort** ist ein Passwort, das vom Benutzer definiert wird (s. Definition eines benutzerdefinierten Passworts auf S. 121);
- **Zufälliges Passwort erstellt mit Hilfe einer Passwortphrase** ist ein Passwort, welches automatisch auf Basis einer Passwortphrase und nach vorgegebenen Parametern erstellt wird (s. Definition des Passworts mit Hilfe einer Passwortphrase auf S. 122);
- **Zufälliges digitales Passwort** ist ein Passwort, welches automatisch aus einer vorgegebenen Zahl von Ziffern erstellt wird (s. Definition eines numerischen Passworts auf S. 123).

3 Klicken Sie auf die Schaltfläche **Passwort ändern**. Führen Sie Abhängigkeit vom gewählten Typ die Aktionen aus, die für den Passwortwechsel erforderlich sind (die Aktionen sind im entsprechenden Unterabschnitt beschrieben).

4 Wenn die Gültigkeitsdauer des neuen Passwortes begrenzt werden soll, aktivieren Sie das Kontrollkästchen **Gültigkeitsdauer des Passwortes beschränken** und geben die gewünschte Anzahl von Tagen ein.

5 Klicken Sie auf **OK**.

Definition eines benutzerdefinierten Passworts

Damit das aktuelle Benutzerpasswort durch ein benutzerdefiniertes Passwort ersetzt wird:

1 Wählen Sie in der Registerkarte **Passwort (s. Abbildung auf S. 120)** die Option **Benutzerdefiniertes Passwort**.

2 Klicken Sie auf **Passwort ändern**.

3 Geben Sie im Fenster **Passwort ändern** das neue Passwort (mindestens 6 Zeichen) in jedem Feld der Reihe nach ein. Beachten Sie dabei die Groß- und Kleinschreibung sowie die aktuelle Tastaturbelegung.



Achtung! Es darf kein Passwort mit einer Länge von 32 Symbolen erstellt werden. Passwörter dieser Länge können in den laufenden Versionen der ViPNet Anwendungen nicht verwendet werden. Diese Einschränkung ist bedingt durch den bestehenden Algorithmus zur Weiterleitung des Passworts an den Cryptoprovider. In Übereinstimmung mit diesem Algorithmus darf die Länge des Passworts nicht mehr als 31 Zeichen betragen.

---

4 Klicken Sie auf **OK**.

Beim Programmstart von ViPNet Business Mail unetr Verwendung des gegebenen Benutzernamens kann nun das neue Passwort eingegeben werden.

Definition des Passworts mit Hilfe einer Passwortphrase

Wenn das laufende Passwort durch ein auf Basis einer Passwortphrase erstelltes zufälliges Passwort getauscht werden soll:

1 Wählen Sie in der Registerkarte **Passwort** (s. Abbildung auf S. 120) die Option **Zufälliges Passwort erstellt mit Hilfe einer Passwortphrase** und geben Sie dann die Parameter des neuen Passwortes ein:

   - Wählen Sie in der Liste **Sprache** die Sprache der Passwortphrase.
   - Wählen Sie in der Liste **Anzahl der Wörter in der Passwortphrase** die Zahl der Worte (3, 4, 6 oder 8), aus denen die Passwortphrase bestehen soll. Je größer die Anzahl der Wörter, desto länger und dementsprechend sicherer wird das Passwort.
   - Wählen Sie in der Liste **Buchstaben aus jedem Wort** die Anzahl der Anfangsbuchstaben eines jeden Wortes (3 oder 4) aus, die das Passwort beinhalten soll.

   In der Zeile **Passwortlänge** wird die Anzahl der Buchstaben im Passwort angezeigt, das anhand der vorgegebenen Parameter erstellt wird.



Achtung! Es darf kein Passwort mit einer Länge von 32 Symbolen erstellt werden. Passwörter dieser Länge können in den laufenden Versionen der ViPNet Anwendungen nicht verwendet werden. Diese Einschränkung ist bedingt durch den bestehenden Algorithmus zur Weiterleitung des Passworts an den Cryptoprovider. In Übereinstimmung mit diesem Algorithmus darf die Länge des Passworts nicht mehr als 31 Zeichen betragen.

2 Klicken Sie auf **Passwort ändern**.

3 Führen Sie die Schritte aus, die im eingeblendeten Fenster **Digitales Roulette** aufgeführt sind.



Hinweis. Wenn das digitale Roulette in der laufenden Sitzung bereits gestartet wurde, wird dieses Fenster nicht angezeigt.

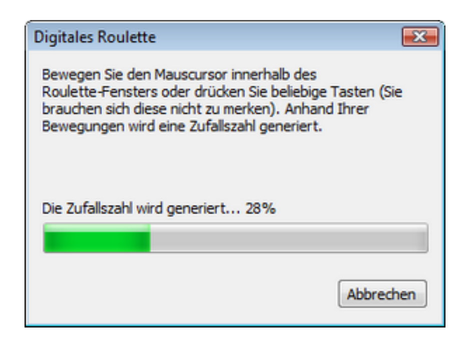


Abbildung 43. Digitales Roulette

4 Merken Sie sich das Passwort und (oder) die Passwortphrase, die im Fenster **Passwort ändern** angezeigt wird.

   Ändern Sie ggf. die Passwortphrase und das Passwort mit Hilfe der Schaltfläche **Nächstes Passwort** entsprechend den angegebenen Parametern.

   Klicken Sie auf **OK**.

Beim Programmstart von ViPNet Business Mail sollten Sie nun dem gleichen Benutzernamen unter Verwendung der englischen Tastaturbelegung die zuvor angegebene Anzahl der Buchstaben eines jeden Wortes der Passwortphrase ohne Leerzeichen eingeben. Beim Programmstart sollte zum Beispiel für die Passwortphrase „Fahrer fuhr toll" bei Verwendung der Standard-Passwortparameter (3 Buchstaben aus jedem Wort) und der englischen Tastaturbelegung die Zeichenfolge „fahfuhtol" eingegeben werden.

Definition eines numerischen Passworts

Damit das aktuelle Benutzerpasswort durch ein numerisches Passwort ersetzt wird:

1 Wählen Sie in der Registerkarte **Passwort** (s. Abbildung auf S. 120) die Option **Zufälliges digitales Passwort** und geben im Feld **Anzahl der Ziffern** die Länge des Passwortes ein.



Achtung! Es darf kein Passwort mit einer Länge von 32 Symbolen erstellt werden. Passwörter dieser Länge können in den laufenden Versionen der ViPNet Anwendungen nicht verwendet werden. Diese Einschränkung ist bedingt durch den bestehenden Algorithmus zur Weiterleitung des Passworts an den Cryptoprovider. In Übereinstimmung mit diesem Algorithmus darf die Länge des Passworts nicht mehr als 31 Zeichen betragen.

2 Klicken Sie auf **Passwort ändern**.

3 Führen Sie die Schritte aus, die im eingeblendeten Fenster **Digitales Roulette** (s. Abbildung auf S. 122) aufgeführt sind.



Hinweis. Wenn das digitale Roulette in der laufenden Sitzung bereits gestartet wurde, wird dieses Fenster nicht angezeigt.

4 Merken Sie sich den numerischen Code, der im Dialogfeld **Passwort ändern** angezeigt wird.

   Ändern Sie ggf. dieses numerisches Passwort mit Hilfe der Schaltfläche **Andere PIN** auf einen anderen Wert, der die gleiche Anzahl an Ziffern besitzt.

   Klicken Sie auf **OK**.

Beim Programmstart von ViPNet Business Mail sollte nun bei Verwendung des gegebenen Benutzernamens das neue numerische Passwort eingegeben werden.

Verschlüsselungsparameter einstellen

Sie können die Verschlüsselungsparameter der ausgehenden Informationen einstellen. Führen Sie dazu die folgenden Schritte durch:

1 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Verschlüsselung**.

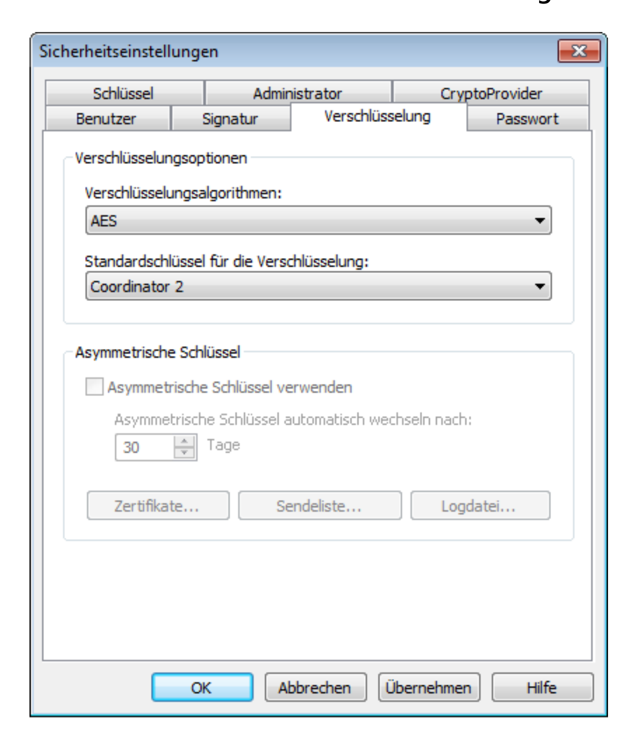


Abbildung 44. Verschlüsselungsparameter einstellen

2 Wählen Sie in der Liste **Verschlüsselungsalgorithmen** den Algorithmus aus, mit dem die ausgehende Nachrichten verschlüsselt werden sollen.

Standardmäßig ist der Algorithmus AES ausgewählt. Die Verschlüsselung ausgehender Nachrichten erfolgt gemäß dem ausgewählten Algorithmus. Die Entschlüsselung eingehender Nachrichten erfolgt gemäß dem Algorithmus, der bei deren Verschlüsselung durch den Absender angegeben wurde.

Wird das Programm ViPNet Network Manager der Version 4.3 und höher oder die Software ViPNet Administrator der Version 4.4.1 und höher zur Verwaltung des ViPNet Netzwerkes verwendet, kann der ViPNet Netzwerkadministrator den Verschlüsselungsalgorithmus ändern. Nach der Aktualisierung der Adresslisten und Schlüssel auf dem Netzwerkknoten wird in diesem Fall der durch den ViPNet Netzwerkadministrator definierte Algorithmus gewählt.

3 Geben Sie in der nachfolgenden Liste die Schlüssel an, mit denen die ausgehende Nachrichten verschlüsselt werden sollen, die mit Hilfe integrierter ViPNet Anwendungen übermittelt werden. Für die Verschlüsselung können sowohl Schlüssel, auf welche nur Sie zugreifen können, als auch Schlüssel, die für die anderen Benutzer Ihres Netzwerkknotens (falls vorhanden) zugänglich sind,

ausgewählt werden. Alle Benutzer, die Zugang zu irgendwelchen Verschlüsselungsschlüsseln haben, werden in der Registerkarte **Benutzer** aufgelistet.

Die Auswahl der Schlüssel für die Verschlüsselung ermöglicht die Abgrenzung des Zugangs unterschiedlicher Benutzer, die auf einem Netzwerkknoten arbeiten, zu den Nachrichten von ViPNet Business Mail. Wenn also für die Verschlüsselung einer ausgehenden Nachricht Schlüssel verwendet wurden, die nur für Sie zugänglich sind, dann können andere Benutzer, die auf Ihrem Netzwerkknoten registriert sind, diese Nachricht nicht lesen.

4 Klicken Sie auf **OK**.

Arbeitsparameter für Cryptoprovider ViPNet einstellen

Im Programm ViPNet Business Mail wird die Software ViPNet CSP verwendet. ViPNet CSP bietet Aufruf kryptographischer Funktionen über die Schnittstelle Microsoft CryptoAPI 2.0. Dies ermöglicht den Aufruf kryptographischer Funktionen aus unterschiedlichen Anwendungen von Microsoft sowie von Drittanbietern, die diese Schnittstelle unterstützen.Außerdem, unterstützt das Programm ViPNet CSP diverse externe Geräte zur Schlüsselspeicherung (s. Externe Datenträger auf S. 174).

Wenn Sie das Programm ViPNet CSP konfigurieren oder die Parameter der automatischen Installation der Zertifikate im System-Zertifikatspeicher einstellen möchten, führen Sie die folgenden Schritte aus:

1 Öffnen Sie die Registerkarte **Cryptoprovider** im Fenster **Sicherheitseinstellungen**.

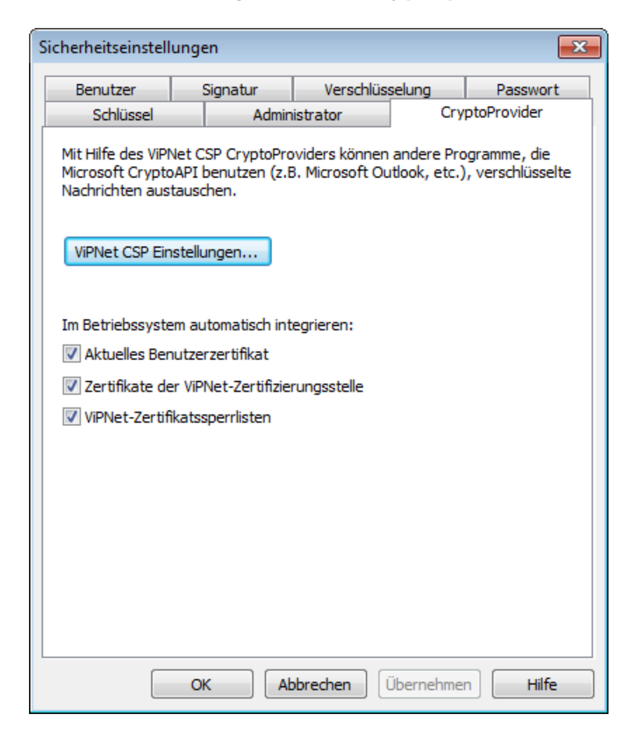


Abbildung 45. Arbeitsparameter für ViPNet CSP einstellen

2 Kilcken Sie auf **ViPNet CSP Einstellungen**, um ViPNet CSP zu konfigurieren. Es wird das Fenster **ViPNet CSP** geöffnet, in dem Sie können:

- Wichtige Cryptoprovider-Parameter definieren;
- Vorgänge mit Schlüsselcontainern durchführen;
- Optionen für die Verwendung externer Datenspeichergeräte konfigurieren: den Typ der Geräte festlegen, die verwendet werden können, eine Initialisierung durchgeführt oder der PIN-Code des Gerätes geändert werden soll.

Informationen an der Arbeit mit dem Programm ViPNet CSP s. im Dokument „ViPNet CSP. Benutzerhandbuch".

3 Aktivieren Sie die erforderlichen Kontrollkästchen, um zu bestimmen, welche Zertifikate, falls sie im Zertifikatspeicher von Windows noch fehlen, automatisch in diesem Zertifikatspeicher installiert werden sollen (s. Zertifikate im Speicher automatisch installieren auf S. 135):
   - **Aktuelles Benutzerzertifikat**, um im Zertifikatspeicher von Windows das als laufendes Zertifikat festgelegte Zertifikat zu installieren;
   - **Zertifikate der ViPNet Key and Certification Authority**, um Herausgeberzertifikate (Stammzertifikate), die vom Programm ViPNet Network Manager oder ViPNet Key and Certification Authority im Zuge von Schlüsselupdates bezogen werden, im Windows-Zertifikatspeicher zu installieren;
   - **ViPNet Zertifikatssperrlisten**, um Zertifikatsperrlisten, die vom Programm ViPNet Network Manager oder ViPNet Key and Certification Authority im Zuge von Schlüsselupdates bezogen werden, im Windows-Zertifikatspeicher zu installieren.
4 Klicken Sie auf **OK**.

8

Arbeit mit den Zertifikaten

Zertifikate anzeigen

Die Anzeige des Zertifikats kann dann erforderlich sein, wenn ausführliche Informationen über das Zertifikat ermittelt werden sollen: Zweck des Zertifikats, sein Herausgeber, die Zusammensetzung der Felder, aus welchem Grund das Zertifikat ungültig ist u. s. w.

Im Programm ViPNet Business Mail können folgende Typen von Zertifikaten angezeigt werden:

- Das laufende Zertifikat des Benutzers (s. Laufendes Benutzerzertifikat anzeigen auf S. 130),
- Persönliche Zertifikate des Benutzers (s. Persönliche Benutzerzertifikate anzeigen auf S. 130),
- Bevollmächtigte Stammzertifikate (s. Vertrauenswürdige Stammzertifikate anzeigen auf S. 131),
- Herausgegebene Zertifikate (s. Herausgegebene Zertifikate anzeigen auf S. 131).

Die wichtigsten Informationen zum ausgewählten Zertifikat werden im Dialogfeld **Zertifikat** in der Registerkarte **Allgemeine** angezeigt:

- Zweck des Zertifikates oder (bei ungültigen Zertifikaten) der Grund für die Ungültigkeit des Zertifikats;
- Name des Subjektes (des Inhabers des öffentlichen Schlüssels), an den das Zertifikat ausgegeben wurde;
- Name des Ausstellers des Zertifikates;
- Laufzeit des Zertifikates;
- Gültigkeitsdauer des privaten Schlüssels, der diesem Zertifikat entspricht;
- Information über die Verwendungsregeln des Zertifikates, die bei Betätigung der Schaltfläche **Notiz des Ausstellers** angezeigt wird.



Hinweis. In einem Zertifikat des Netzwerkes auf Basis der Software ViPNet Administrator ist die Schaltfläche **Notiz des Ausstellers** erst dann verfügbar, wenn dem Zertifikat bei seiner Erstellung im Programm ViPNet Key and Certification Authority die entsprechenden Anwendungsregeln zugeordnet worden sind.

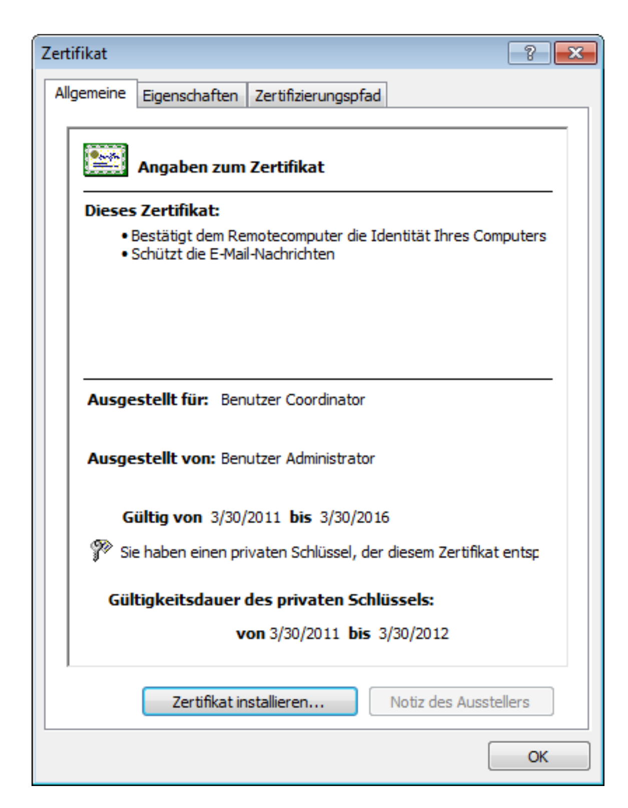


Abbildung 46. Wichtigste Informationen zum Zertifikat anzeigen

Laufendes Benutzerzertifikat anzeigen

Um das laufende Benutzerzertifikat anzeigen zu lassen:

1 Wählen Sie den Menüpunkt **Extras** und in diesem den Befehl **Sicherheitseinstellungen**.

2 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**, betätigen Sie danach die Schaltfläche **Details**.

Das Fenster **Zertifikat** mit Information über das laufende Zertifikat wird geöffnet.

Persönliche Benutzerzertifikate anzeigen

Um die persönlichen Benutzerzertifikate anzeigen zu lassen:

1 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**, betätigen Sie danach die Schaltfläche **Zertifikate**.

Das Fenster **Zertifikatmanager** mit Informationen über alle persönlichen Benutzerzertifikate sowie über die im Betriebssystem installierten Zertifikate wird geöffnet. Alle diese Zertifikate sind initialisiert.



Hinweis. Die im Betriebssystem installierten Zertifikate werden dann angezeigt, wenn in der Registerkarte **Administrator** des Dialogfeldes Sicherheitseinstellungen das Kontrollkästchen **Verwendung externer Zertifikate erlauben** (s. Zusätzliche Sicherheitseinstellungen auf S. 115) gesetzt ist.

2 Sollten nähere Informationen zu einem der Zertifikate erforderlich sein, wählen Sie das entsprechende Zertifikat aus, betätigen Sie die Schaltfläche **Eigenschaften** oder doppelklicken Sie auf das Zertifikat.

Das Fenster **Zertifikat** mit Informationen über das ausgewählte persönliche Zertifikat wird geöffnet.

Vertrauenswürdige Stammzertifikate anzeigen

Um vertrauenswürdige Stammzertifikate anzeigen zu lassen:

1 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**, betätigen Sie danach die Schaltfläche **Zertifikate**.

2 Öffnen Sie im Fenster **Zertifikatmanager** die Registerkarte **Vertrauenswürdige Stammzertifikate**.

3 Sollten nähere Informationen zu einem der Zertifikate erforderlich sein, wählen Sie das entsprechende Zertifikat aus und betätigen Sie die Schaltfläche **Eigenschaften** oder doppelklicken Sie auf das Zertifikat.

Das Fenster **Zertifikat** mit Informationen über das ausgewählte Stammzertifikat wird geöffnet.

Herausgegebene Zertifikate anzeigen

Um die herausgegebenen Zertifikate anzeigen zu lassen:

1 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**, betätigen Sie danach die Schaltfläche **Ausgestellte Zertifikate**.

Nun öffnet sich das Fenster **Zertifikatmanager**, das Informationen über Zertifikate enthält, die im Programm ViPNet Key and Certification Authority auf Benutzeranfrage oder auf Anfrage des Administrators des Programms ViPNet Key and Certification Authority erstellt, jedoch noch nicht initialisiert wurden.

2 Sollten nähere Informationen zu einem der Zertifikate erforderlich sein, wählen Sie das entsprechende Zertifikat aus und betätigen Sie die Schaltfläche **Eigenschaften** oder doppelklicken Sie auf das Zertifikat.

Das Fenster **Zertifikat** mit Informationen über das ausgewählte herausgegebene Zertifikat wird geöffnet.

Zertifizierungskette anzeigen

Um die Zertifizierungskette (auf S. 180) anzeigen zu lassen:

1. Rufen Sie das Fenster **Zertifikat** für das Zertifikat, für welches die Kette angezeigt werden soll.
2. Öffnen Sie die Registerkarte **Zertifizierungsweg**.

   In dieser Registerkarte werden Zertifikate angezeigt, die eine Hierarchie der Herausgeber des Zertifikates bilden, für welches das Fenster **Zertifikat** aufgerufen wurde, zusammen mit deren Statusinformation.
3. Sollten nähere Informationen zum Zertifikat eines der Herausgeber erforderlich sein, wählen Sie das entsprechende Zertifikat aus und klicken auf **Zertifikat anzeigen** oder doppelklicken auf das Zertifikat. Das Fenster **Zertifikat** mit Information über das ausgewählte Zertifikat wird geöffnet.

Zertifikatfelder anzeigen und Zertifikat ausdrucken

Um die Felder eines bestimmten Zertifikates anzeigen zu lassen:

1. Rufen Sie das Fenster **Zertifikat** für das Zertifikat auf, dessen Feld angezeigt werden soll.
2. Öffnen Sie die Registerkarte **Eigenschaften**.

   Standardmäßig wird in dieser Registerkarte eine Auflistung aller Felder angezeigt, die diesem Zertifikat bei seiner Erstellung im Programm ViPNet Network Manager oder ViPNet Administrator Key and Authority Center zugeordnet wurden.
3. Wählen Sie in der Pop-up-Liste **Anzeigen** die benötigte Gruppe von Feldern aus, um die Menge der angezeigten Felder einzuschränken:
   - **Nur die Datenfelder der Version 1**, d.h. alle Felder außer den Erweiterungen;
   - **Nur die Erweiterungen**, d.h. zusätzliche Felder des Zertifikates, die dem Standard X.509 Version 3 entsprechen;



Hinweis. Die Erweiterung **Gültigkeitsdauer des privaten Schlüssels** wird in dem Fall angezeigt, wenn die Laufzeit des Zertifikates länger als 1 Jahr ist. Wenn die Gültigkeitsdauer des Zertifikats 1 Jahr übersteigt, beträgt die Laufzeit des privaten Schlüssels genau 1 Jahr.

   - **Nur kritische Erweiterungen**, d.h. nur die Erweiterungen, die vom Herausgeber als kritisch angesehen werden;
   - **Nur die Eigenschaften**, d.h. die Parameter, die keine Zertifikatsfelder sind und dem Zertifikat zugeordnet werden, wenn es im Systemspeicher der Arbeitsstation aufbewahrt wird.
4. Wählen Sie in der Tabelle das gewünschte Feld aus und sehen Sie sich im unteren Bereich des Dialogfeldes den Inhalt an.

Um das Zertifikat auf dem für diese Arbeitsstation aktuellen Drucker auszudrucken, betätigen Sie die Schaltfläche **Drucken**.

Zertifikate verwalten

Die Möglichkeiten des Programms ViPNet Business Mail bei der Verwaltung von Zertifikaten mit Hilfe des Fensters **Sicherheitseinstellungen** sind in der nachfolgenden Tabelle vorgestellt.

Funktionelle Möglichkeit	Link
Installation der Zertifikate im Speicher. Es ist möglich, die Parameter sowohl für eine automatische Installation der Zertifikate im Speicher als auch für eine manuelle Installation zu konfigurieren.	Zertifikate im Speicher automatisch installieren (auf S. 135) Zertifikate im Speicher manuell installieren (auf S. 137)
Wechsel des laufenden Zertifikats. Es kann ein anderes Zertifikat (aus der Menge der gültigen persönlichen Benutzerzertifikate) als laufendes Zertifikat festgelegt werden.	Laufendes Zertifikat wechseln (auf S. 143)
Aktualisierung des privaten Schlüssels und des Zertifikats. Es können Parameter für eine automatische Benachrichtigung über den Ablauf der Gültigkeitsdauer des aktuellen Zertifikats und des passenden privaten Schlüssels konfiguriert werden, und, wenn nötig, eine Aktualisierungsanfrage für dieses Zertifikat und den privaten Schlüssel erstellt werden.	Meldung über Ablauf des privaten Schlüssels und Zertifikat einstellen (auf S. 145) Verfahren zum Erneuern des privaten Schlüssels und Zertifikats (auf S. 146)
Initialisierung der Zertifikate. Um das übermittelte Zertifikat zu verwenden, muss dieses Zertifikat zunächst initialisiert werden. Es können entweder Parameter für eine automatische Initialisierung der Zertifikate konfiguriert werden, oder die Initialisierung kann manuell durchgeführt werden.	Zertifikat initialisieren (auf S. 151) Zertifikate automatisch initialisieren (auf S. 151) Zertifikate manuell initialisieren (auf S. 151) RSA Zertifikate installieren (auf S. 140)
Anzeigen und Löschen von Zertifikatsanfragen. Es kann der Status der Zertifikatsanfragen, die vom aktuellen Benutzer erstellt wurden, angezeigt werden. Nicht benötigte Anfragen können gelöscht werden.	Arbeiten mit Zertifikatsanfragen (auf S. 152) Zertifikatsanfrage anzeigen (auf S. 152) Zertifikatsanfrage löschen (auf S. 153)
Export der Zertifikate. In Abhängigkeit vom Verwendungszweck des Zertifikats außerhalb der ViPNet Software kann das Zertifikat in Dateien unterschiedlicher Formate exportiert werden.	Zertifikat exportieren (auf S. 153)

Zertifikate im Speicher installieren

Durch Installation der Zertifikate im Speicher ist es möglich, die Zertifikate in externen Applikationen zu verwenden (wie z.B. Windows Live Mail, Microsoft Outlook, Microsoft Word u.a.). Sie können das Zertifikat im Speicher des Betriebssystems oder im Speicher des Programms ViPNet Business Mail (Ordner `D_STATION` des Installationsordners) installieren.

Die Installation kann automatisch oder manuell vorgenommen werden.



Achtung! Bei der Installation des Zertifikates im Betriebssystem Windows Vista oder Windows Server 2008 ist das Programm ViPNet Business Mail unter dem Namen des Administrators des Betriebssystems zu starten (mit dem Befehl **Als Administrator starten (Run as Administrator)**) im Kontextmenü der Verknüpfung.

Zertifikate im Speicher automatisch installieren

Die Installation der Zertifikate wird bei Einhaltung der beiden folgenden Bedingungen automatisch gestartet:

- Die Zertifikate (das laufende Benutzerzertifikat, das Stammzertifikat und die Listen der abgerufenen Zertifikate) sind im Speicher nicht vorhanden.
- Im Fenster **Sicherheitseinstellungen** sind in der Registerkarte **Cryptoprovider** die Kontrollkästchen der Gruppe **Im Betriebssystem automatisch integrieren** deaktiviert.



Hinweis. Im automatischen Modus wird die Installation der Zertifikate im Speicher des aktuellen Benutzers vorgenommen.

Zur automatischen Installation des laufenden Benutzerzertifikates und der Listen der widerrufenen Zertifikate (unter Einhaltung der o.g. Bedingungen) sind keine weiteren Aktionen seitens des Benutzers erforderlich.

Es sollte beachtet werden, dass die automatische Installation des Stammzertifikats eine längere Zeit in Anspruch nehmen kann, abhängig davon, welches ViPNet Programm dafür verwendet wird:

- Im Programm ViPNet Monitor wird die Parameterabfrage fünf Minuten nach dem Start des Programms und anschließend in 2-Stunden-Intervallen durchgeführt. Falls das Fenster **Sicherheitseinstellungen** geöffnet bleibt, verkürzt sich das Abfrageintervall auf 10 bis 15 Minuten.
- In den Programmen ViPNet Business Mail und ViPNet Cryptoservice wird die Parameterabfrage in Intervallen von 30 bis 60 Minuten durchgeführt.

Um das Stammzertifikat automatisch zu installieren:

1 Wenn das Fenster **Installation des Stammzertifikats** erscheint:



Hinweis. Das Fenster **Installation des Stammzertifikats** wird dann eingeblendet, wenn das Stammzertifikat im Zertifikatspeicher von Windows fehlt. Das kann unter folgenden Umständen der Fall sein:

- Beim ersten Start der ViPNet Software nach der Installation des Netzwerkknotens.
- Wenn ein Update für das aktuelle Benutzerzertifikat erhalten wurde, das ein neues Stammzertifikat enthält.

- Sollte die automatische Installation des Stammzertifikates erforderlich sein, klicken Sie auf **OK**.
- Sollte keine automatische Installation des Stammzertifikates und anderer Zertifikate erforderlich sein, aktivieren Sie das Kontrollkästchen **Automatische Zertifikatsinstallation deaktivieren** und anschließend klicken Sie auf **OK**;



Hinweis. Im Fenster **Sicherheitseinstellungen** in der Registerkarte **Cryptoprovider** werden auch die Kontrollkästchen **Im Betriebssystem automatisch integrieren** deaktiviert.

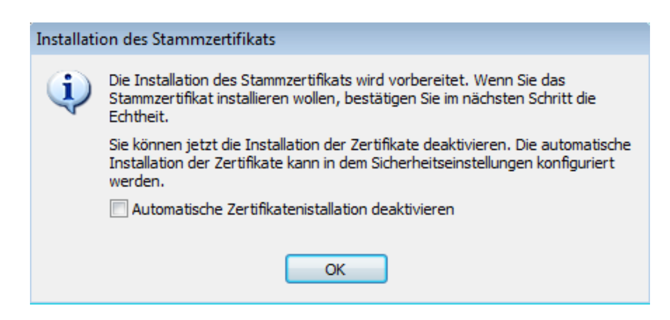


Abbildung 47. Installation des Stammzertifikates

2 Wurde die automatische Installation der Zertifikate nicht abgebrochen, prüfen Sie im Dialogfeld der Anfrage auf Hinzufügung des Zertifikates in den Speicher die Echtheit des Zertifikates und klicken dann auf **Ja**.

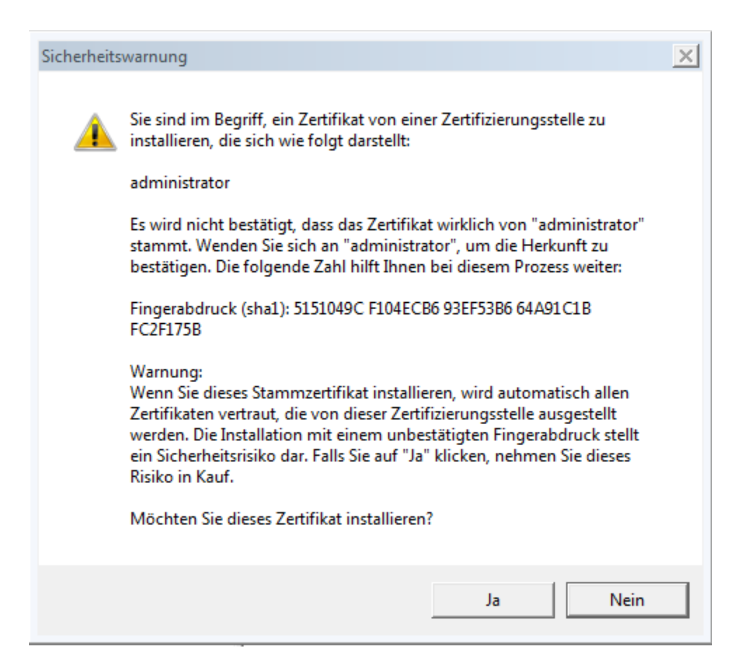


Abbildung 48. Echtheitsbestätigung des Stammzertifikates

Das Stammzertifikat ist im Speicher für die Zertifikate des laufenden Benutzers installiert.

Zertifikate im Speicher manuell installieren

Um mit geschützten Dokumenten zu arbeiten, müssen ein privater Schlüssel und ein ihm entsprechendes Zertifikat vorhanden sein. Die Installation des Schlüssels und des Zertifikates kann durch Installation eines Containers oder durch Installation des Zertifikates und des Containers des privaten Schlüssels einzeln vorgenommen werden.

Liegt Ihnen der private Schlüssel vor und müssen Sie auf dessen Basis ein Zertifikat erstellen oder ein bestehendes Zertifikat aktualisieren, richten Sie eine Zertifikatsanfrage an die Zertifizierungsstelle.



Achtung! Um mit geschützten Dokumenten arbeiten zu können, muss im Speicher außer dem Benutzerzertifikat auch das Stammzertifikat des Herausgebers und die Zertifikatsperrliste installiert sein.

Das Zertifikat kann gesondert installiert und dem persönlichen privaten Schlüssel zugeordnet werden.

Um das Zertifikat im Betriebssystem zu installieren:

1. Rufen Sie das Fenster **Zertifikat** für das Zertifikat auf, welches installiert werden soll (s. Zertifikate anzeigen auf S. 129).
2. Betätigen Sie die Schaltfläche **Zertifikat installieren**.
3. Betätigen Sie auf der Startseite des Installationsassistenten die Schaltfläche **Weiter**.
4. Geben Sie auf der Seite **Zertifikatspeicher definieren** an, in welchem Speicher Ihr Zertifikat installiert werden soll und klicken auf **Weiter**.

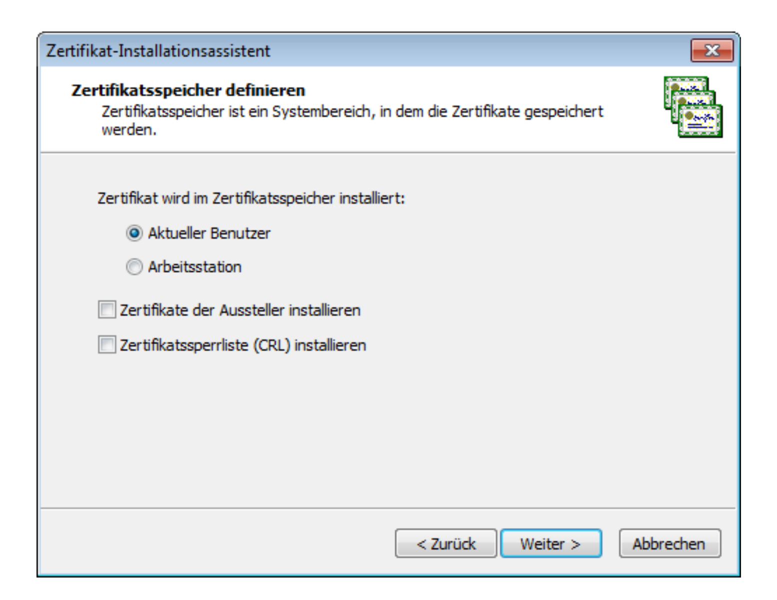


Abbildung 49. Zertifikatspeicher auswählen



Hinweis. Das Zertifikat ist im Speicher des laufenden Benutzers für die Ver- und Entschlüsselung, die Signierung von Dateien und für den Zugriff auf geschützte Ressourcen über den Browser zu installieren. Im Speicher des Computers sollten nur diejenigen Zertifikate installiert werden, die von den Diensten dieses Computers verwendet werden.

Das Zertifikat für das Produkt ViPNet CSP ist im Rechnerspeicher unter Einsatz von ViPNet CSP auf dem Web-Server zur Gewährleistung des Zugangs zu den geschützten Ressourcen zu installieren.

Wenn die Option, das Zertifikat im Rechnerspeicher zu installieren, nicht verfügbar ist, melden Sie sich im System mit Administratorrechten an.

5 Auf der Seite **Status der Zertifikat-Installation**:

- Prüfen Sie die Richtigkeit der ausgewählten Parameter. Kehren Sie ggf. mit der Schaltfläche **Zurück** zur vorherigen Seite des Assistenten zurück und wählen Sie andere Parameter aus.



Abbildung 50. Die Seite „Status der Zertifikat-Installation“

- Wird das Zertifikat in der Datei getrennt von dem privaten Schlüssel aufbewahrt, aktivieren Sie das Kontrollkästchen **Container mit dem privatem Schlüssel definieren**.



Hinweis. Das Kontrollkästchen **Container mit dem privatem Schlüssel definieren** muss nicht unbedingt aktiviert werden. In diesem Fall muss, nachdem der Installationsassistent für Zertifikate beendet ist, der Speicherort des Containers angegeben werden.

- Klicken Sie auf **Weiter**.

6 Wenn das Kontrollkästchen **Container mit dem privatem Schlüssel definieren** aktiviert ist und der Container nicht gefunden wurde oder nicht verfügbar ist, geben Sie im sich öffnenden Dialogfenster **Initialisierung des Schlüsselcontainers** den Speicherort des Containers des privaten Schlüssels an:

- Ordner auf der Festplatte;
- Gerät mit Angabe seiner Parameter und des PIN-Codes.



Hinweis. Um ein externes Gerät verwenden zu können, müssen der Treiber dieses Gerätes installiert sein. Die Übersicht über die verfügbaren Datenträger sowie nützliche Information zu deren Verwendung ist im Bereich Externe Datenträger (auf S. 174).

Anschließend klicken Sie auf **OK**.

7 Klicken Sie im Dialogfeld „Möchten Sie das Zertifikat im Container mit privaten Schlüssel speichern?“ auf **Ja**, um das Zertifikat dem Container des privaten Schlüssels hinzuzufügen oder **Nein**, um das Zertifikat als gesonderte Datei zu belassen.



Tipp. Es ist zweckmäßig, das Zertifikat im gleichen Container mit dem privaten Schlüssel abzuspeichern, wenn der Container übertragen und auf einem anderen Rechner installiert werden soll.

8 Wenn das Kontrollkästchen **Container mit dem privatem Schlüssel definieren** aktiviert und der Container verfügbar ist, geben Sie in dem sich öffnenden Dialogfeld **ViPNet CSP - Passwort des Schlüsselcontainers** im Feld **Passwort** das Zugangspasswort für den Container ein und klicken danach auf **OK**.



Hinweis. Das Dialogfeld **ViPNet CSP** - **Passwort des Schlüsselcontainers** wird dann nicht angezeigt, wenn zuvor ein Passwort gespeichert und das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen** aktiviert wurde.

9 Auf der Seite **Zertifikat-Installationsassistent wird beendet** klicken Sie auf **Fertig**.

Das Zertifikat wurde im gewählten Zertifikatspeicher installiert. Wenn im Zuge der Installation dem Zertifikat kein privater Schlüssel gegenübergestellt wurde, dann muss ein dem Zertifikat entsprechender Schlüsselcontainer (s. Schlüsselcontainer installieren auf S. 162) installiert werden.

RSA Zertifikate installieren

RSA-Zertifikate werden in ViPNet Netzwerken in PFX Containern verteilt und aus eine besondere Art und Weise installiert. Damit Sie ein RSA-Zertifikat in ViPNet Business Mail verwenden können, sollte Ihr ViPNet Netzwerkadministrator Ihnen eine `*.pfx` Datei mit einem RSA-Zertifikat senden. Er kann diese Datei an Ihren Netzwerkknoten entweder zusammen mit Aktualisierungen für Schlüsseldistributionen senden oder eine Schlüsseldistribution mit einer `*.pfx` Datei zur Verfügung stellen.



Achtung! Sie können keine Anträge auf Zertifikatserneuerung für RSA-Zertifikate machen.

Innerhalb weniger Minuten nachdem Ihr ViPNet Netzwerkknoten die Updates für Schlüsseldistributionen erhalten hat, oder nachdem Sie eine neue Schlüsseldistribution (`*.dst` Datei) manuell installiert haben, öffnet sich ein Fenster mit der Frage, ob Sie das neue Zertifikat installieren möchten.

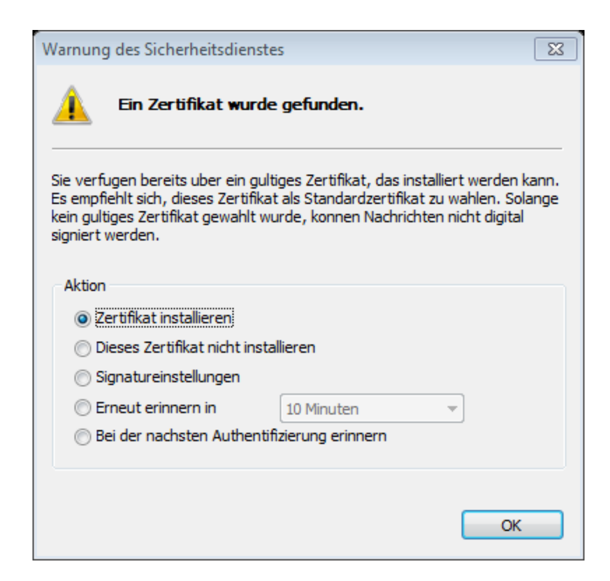


Abbildung 51. RSA-Zertifikat wurde gefunden

Um das Zertifikat zu installieren, gehen Sie wie folgt vor:

1 Wählen Sie im geöffneten Fenster **Warnung des Sicherheitsdienstes** den Eintrag **Zertifikat installieren** und klicken auf **OK**.

2 Geben Sie im geöffneten Fenster das Passwort, das für Ihren ViPNet Netzwerkknoten in ViPNet Administrator definiert wurde, ein und klicken auf **OK**, um das Zertifikat zu installieren.

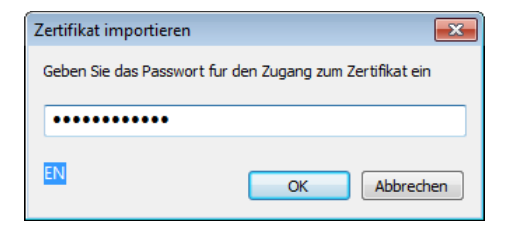


Abbildung 52. Das Fenster Zertifikatspasswort

Ist das eingegebene Passwort richtig, wird Ihr Zertifikat in ViPNet Business Mail installiert. Das Aussteller-Zertifikat und die Zertifikatssperrliste werden aus dem PFX Container installiert.

Stimmt das eingegebene Passwort mit dem für Ihren Netzwerkknoten in ViPNet Administrator definierten Passwort nicht überein, wird das Zertifikat nicht installiert und die `*.pfx` Datei wird automatisch in den ViPNet Business Mail Installationsordner, in den Benutzerschlüsselunterordner `\user_AAAA\key_disk\dom` (wobei `AAAA` eine hexadezimale ID eines ViPNet Benutzers ohne Netzwerknummer ist) gespeichert. Sie können in diesem Fall das Zertifikat manuell installieren, indem Sei die Datei `*.pfx` verwenden.



Hinweis. Damit ViPNet Business Mail ein RSA Zertifikat aus dem Zertifikatsspeicher des Betriebssystems importieren kann, sollte im Fenster **Sicherheitseinstellungen** in der Registerkarte **Administrator** das Kontrollkästchen **Zertifikate aus dem Zertifikatsspeicher des Betriebssystems erlauben** aktiviert werden.

Um das Zertifikat aus der `*.pfx` Datei in ViPNet Business Mail manuell zu importieren, gehen Sie wie folgt vor:

1 Öffnen Sie den Ordner mit der `.pfx` Datei im Windows Explorer.

2 Starten Sie den Zertifikatsimport-Assistenten mit einem Doppelklick auf die `*.pfx` Datei und folgen den Anweisungen des Assistenten.

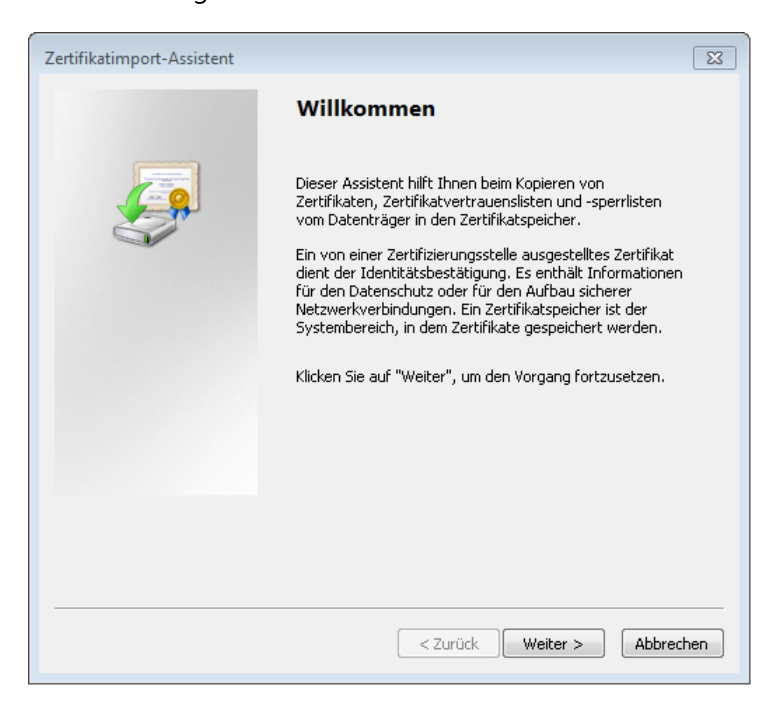


Abbildung 53. Den Zertifikatsimport-Assistenten starten

3 Wenn der Assistent von Ihnen verlangt, das Passwort für den privaten Schlüssel einzugeben, geben Sie das Passwort, das für Ihren ViPNet Netzwerkknoten in ViPNet Administrator Key and Certification Authority definiert wurde, ein.

4 Klicken Sie auf **Beenden** auf der letzten Seite des Assistenten, um das Zertifikat in den Zertifikatsspeicher Ihres Betriebssystems zu importieren.

5 Wählen Sie in ViPNet Business Mail **Extras** > **Sicherheitseinstellungen**.

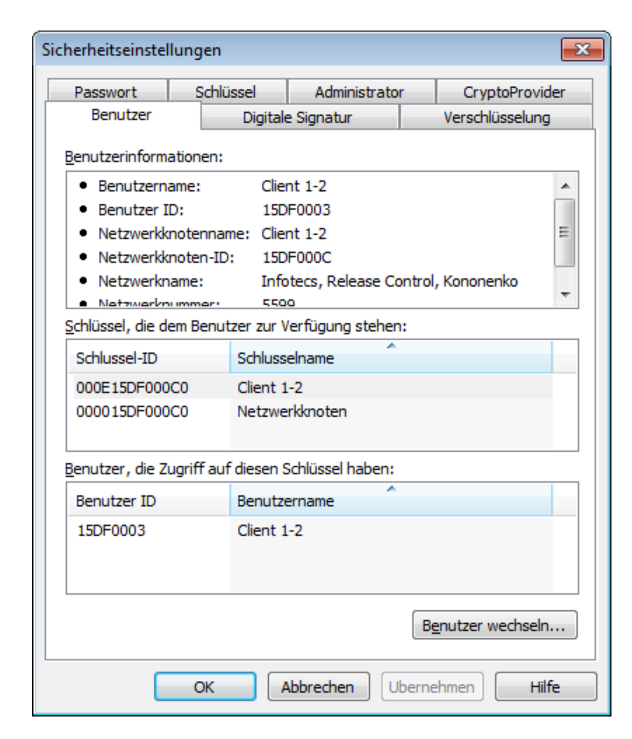


Abbildung 54. RSA Zertifikat des öffentlichen Schlüssels manuell installieren

6 Klicken Sie im geöffneten Fenster in der Registerkarte **Signatur** auf **Ändern** und wählen das Zertifikat, das Sie verwenden möchten, aus. Wollen Sie Informationen zum Zertifikat vor der Installation abrufen, klicken Sie auf **Eigenschaften**.

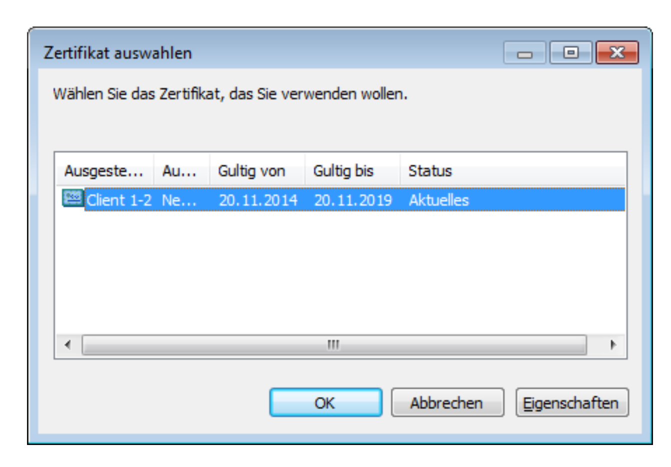


Abbildung 55. Zertifikat auswählen

7 Klicken Sie auf **OK**, um das Zertifikat in ViPNet Business Mail zu installieren.

Laufendes Zertifikat wechseln

Haben Sie mehrere laufende persönliche Zertifikate, so können Sie ein beliebiges davon als laufendes Zertifikat verwenden.



Achtung! Wenn bei einer Zertifikatsaktualisierung das neue, auf Benutzeranfrage ausgestellte Zertifikat auf den Netzwerkknoten zusammen mit den Benutzerschlüsseln übermittelt wurde, dann muss dieses Zertifikat für die weitere Verwendung zunächst als aktuelles Zertifikat festgelegt werden.

Um ein Zertifikat als das gültige persönliche laufende Zertifikat zu bestimmen:

1 Im Fenster **Sicherheitseinstellungen** öffnen Sie die Registerkarte **Signatur** und betätigen Sie danach die Schaltfläche **Auswählen**.

   Liegt Ihnen mindestens ein persönliches Zertifikat vor, so erscheint das Fenster **Zertifikat auswählen** mit der Information über alle persönlichen Zertifikate und über die Zertifikate, die im Betriebssystemspeicher installiert sind.



Hinweis. Die im Betriebssystem installierten Zertifikate werden dann angezeigt, wenn in der Registerkarte **Administrator** des Dialogfeldes Sicherheitseinstellungen das Kontrollkästchen **Verwendung externer Zertifikate erlauben** (s. Zusätzliche Sicherheitseinstellungen auf S. 115) gesetzt ist.

   Wird kein gültiges persönliches Zertifikat gefunden, so erscheint ein Dialogfeld mit der Meldung „Keine gültigen Zertifikate mit gültigem privaten Schlüssel“.

2 Wählen Sie im Fenster **Zertifikat auswählen** das benötigte Zertifikat aus, indem Sie ggf. die Schaltfläche **Eigenschaften** zur Anzeige detaillierter Informationen zum Zertifikat betätigen und danach auf **OK** klicken.



Hinweis. Als laufendes Zertifikat kann nur ein initialisiertes Zertifikat verwendet werden. Ein herausgegebenes und nicht initialisiertes Zertifikat muss zuerst initialisiert und dann als laufendes Zertifikat definiert werden.

Nach erfolgreicher Ausführung der beschriebenen Schritte kann das ausgewählte Zertifikat als laufendes Zertifikat festgelegt werden. Dabei ändert sich in der Registerkarte **Schlüssel** (s. Abbildung auf S. 158) in Gruppe **Signatur** die Information über den Schlüsselcontainer, in welchem das gewählte Zertifikat gespeichert ist.

Private Schlüssel und Zertifikat erneuern

Das Zertifikat des öffentlichen Schlüssels und der private Schlüssel haben eine beschränkte Gültigkeitsdauer, deswegen sollten sie regelmäßig aktualisiert werden. Bei der Aktualisierung des Zertifikats wird der private Schlüssel ebenfalls aktualisiert.

Die Aktualisierung des Zertifikats und des zum Zertifikat passenden privaten Schlüssels sollte in folgenden Fällen durchgeführt werden:

- Die Gültigkeitsdauer des Zertifikats mit dem öffentlichen Schlüssel ist abgelaufen. Die Gültigkeitsdauer des Zertifikats kann bis zu 5 Jahre betragen.
- Die Gültigkeitsdauer des privaten Schlüssels ist abgelaufen. Die Gültigkeitsdauer des privaten Schlüssels beträgt 1 Jahr (wenn die Gültigkeitsdauer des Zertifikats 1 Jahr übersteigt) oder entspricht der Gültigkeitsdauer des Zertifikats (wenn die Gültigkeitsdauer des Zertifikats weniger als 1 Jahr beträgt).
- Es sollte ein Zertifikat angefordert werden, in dem die Besitzerdaten (Position, Abteilungen und andere) geändert oder zusätzliche Attribute oder Erweiterungen hinzugefügt sind. Zum Beispiel können dem Zertifikat bestimmte Anwendungsrichtlinien hinzugefügt werden, um es für den Einsatz in einem Dokumentenmanagement-System vorzubereiten.

Auf diese Weise sollten das Zertifikat des öffentlichen Schlüssels und der private Schlüssel nicht seltener als einmal im Jahr aktualisiert werden.

Das Zertifikat und der private Schlüssel können nicht nur im Programm ViPNet Business Mail (Fenster **Sicherheitseinstellungen**), sondern auch mit Hilfe der Programmkomponente ViPNet CSP aktualisiert werden (s. Dokument „ViPNet CSP. Benutzerhandbuch“).



Hinweis. Wenn die Gültigkeitsdauer des privaten Schlüssels abgelaufen ist, das Zertifikat des offenen Schlüssels dabei aber gültig bleibt, kann eine Zertifikatsanfrage erstellt werden. Die Anfrage wird mit dem privaten Schlüssel signiert, die Signatur wird aber ungültig sein. Diese Signatur wird nicht zur Bestätigung der Urheberschaft verwendet, sie wird lediglich zur Prüfung der Integrität der Anfrage benutzt. In diesem Fall ist eine Bestätigung der Richtigkeit der Anfrage in Übereinstimmung mit den in der Zertifizierungsstelle angenommenen Vorschriften erforderlich.

Nach Ablauf der Gültigkeitsdauer des privaten Schlüssels oder des Zertifikats kann keine Aktualisierungsanfrage mehr erzeugt werden. Ein neues Zertifikat kann nur auf Initiative des Administrators des Programms ViPNet Key and Certification Authority herausgegeben werden.

Meldung über Ablauf des privaten Schlüssels und Zertifikat einstellen

Standardmäßig warnt die Software ViPNet Business Mail 15 Tage bevor die Laufzeit des privaten Schlüssels oder des Zertifikats abläuft.

Um die Benachrichtigung einzustellen, gehen Sie wie folgt vor:

1. Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**.

   Im Feld **Aktuelles Zertifikat** ist die Gültigkeitsdauer des Zertifikates angegeben.

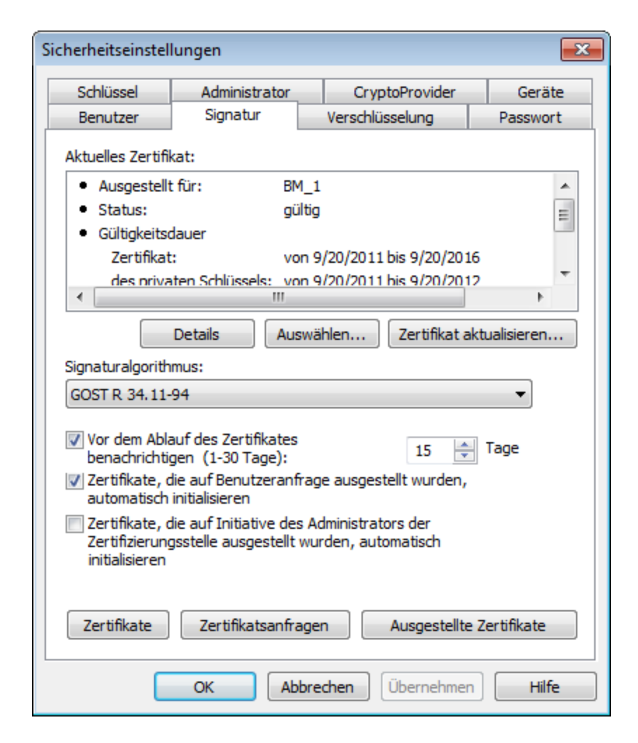


Abbildung 56. Die Registerkarte „Signatur"

2 Aktivieren oder deaktivieren Sie in der Gruppe **Zusätzlich** das Kontrollfeld **Vor dem Ablauf des Zertifikates benachrichtigen** und geben Sie im Feld rechts die Anzahl der Tage ein (max. 30).

Verfahren zum Erneuern des privaten Schlüssels und Zertifikats

Es ist erforderlich, einige Tage vor dem Ablauf des Zertifikates folgende Schritte durchzuführen:

- Ist die Benachrichtigung über den Ablauf des Zertifikates aktiv:
  - Bei Erreichen der voreingestellten Anzahl von Tagen bis zum Ablauf des Zertifikates gibt das Programm ViPNet Business Mail eine entsprechende Meldung heraus.

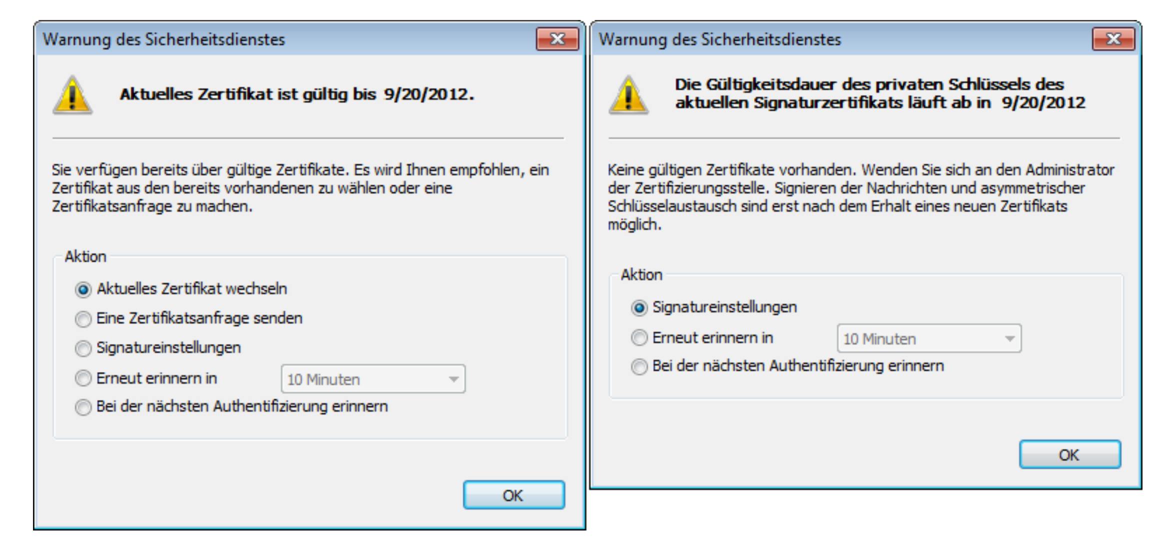


Abbildung 57. Meldungen über das ablaufende Zertifikat und den privaten Schlüssel

- Wenn ein Zertifikat abläuft, wählen Sie im Fenster der Meldung **Eine Zertifikatsanfrage senden** und klicken auf **OK**. Der **Assistent zur Zertifikataktualisierung** wird gestartet.



Hinweis. Sie können auch die Signatureinstellungen öffnen oder den Versand der Erneuerungsanfrage für das Zertifikat aufschieben.

- Wenn ein privater Schlüssel abläuft, wählen Sie im Fenster die Meldung **Signatureinstellungen** und klicken auf **OK**. Klicken Sie im eingeblendeten Fenster **Sicherheitseinstellungen** in der Registerkarte **Signatur** auf **Zertifikat aktualisieren**.

- Ist die Benachrichtigung über den Ablauf des Zertifikates nicht aktiv:
  - Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**.
  - Klicken Sie in der Registerkarte **Signatur** (s. Abbildung auf S. 146) auf **Zertifikat aktualisieren**. Der **Assistent zur Zertifikataktualisierung** wird gestartet.

Um die Anfrage zur Erneuerung des Zertifikats mit Hilfe des Assistenten zu erstellen und zu senden:

1 Klicken Sie auf der Startseite des Assistenten auf **Weiter**.



Abbildung 58. Startseite des Zertifikatsaktualisierungs-Assistenten

2 Auf der Seite **Öffentlicher Schlüssel** führen Sie folgende Aktionen durch:

2.1 Geben Sie der Geltungsbereich des Schlüssels und des Zertifikats:

- den Wert **Signatur** wenn das Zertifikat nur für Signatur verwendet werden soll;
- den Wert **Signatur und Verschlüsselung**, wenn das Zertifikat sowohl für Signatur als auch für Verschlüsselung benutzt werden soll.

2.2 Geben Sie der Algorithmus der Schlüsselgenerierung und Parameter des Algorithmus.

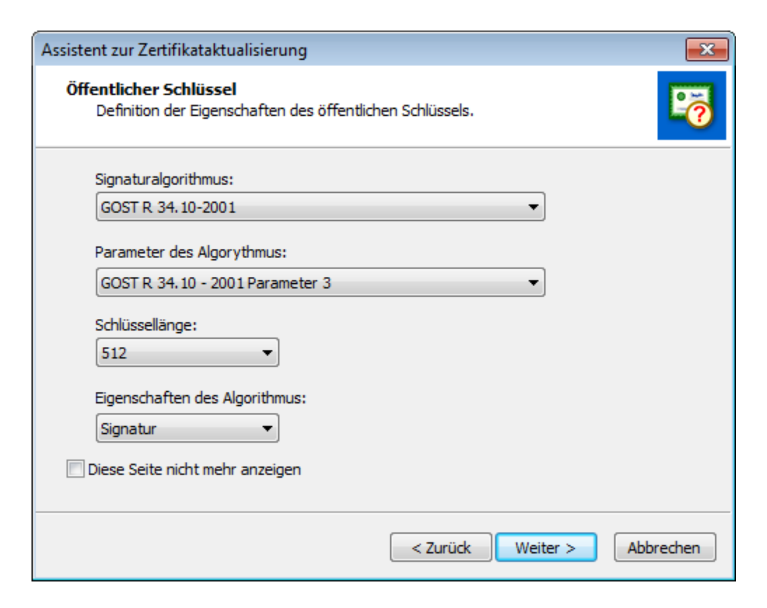


Abbildung 59. Parameter des öffentlichen Schlüssels auswählen

2.3 Klicken Sie auf **Weiter**.

3 Geben Sie auf der Seite **Container mit privatem Schlüssel** den Speicherplatz des Containers mit dem privaten Schlüssel an:

- den Ordner auf der Festplatte,
- das Gerät mit Angabe seiner Parameter und des PIN-Codes.



Hinweis. Um ein externes Gerät verwenden zu können, müssen der Treiber dieses Gerätes installiert sein. Die Übersicht über die verfügbaren Datenträger sowie nützliche Information zu deren Verwendung ist im Bereich Externe Datenträger (auf S. 174).

Anschließend klicken Sie auf **Weiter**.

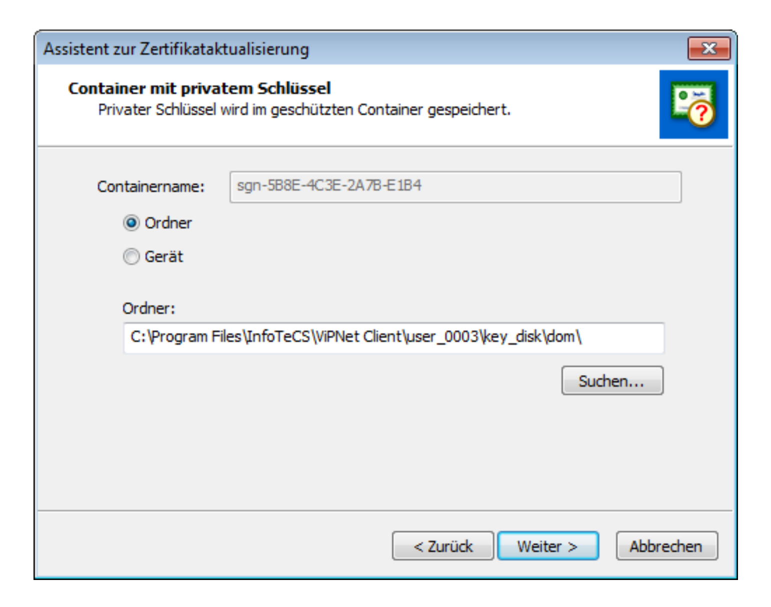


Abbildung 60. Speicherort des Containers mit privatem Schlüssel angeben

4 Geben Sie auf der Seite **Zertifikat gültig** bis die gewünschte Gültigkeitsdauer des zu erneuernden Zertifikates an und klicken danach auf **Weiter**.

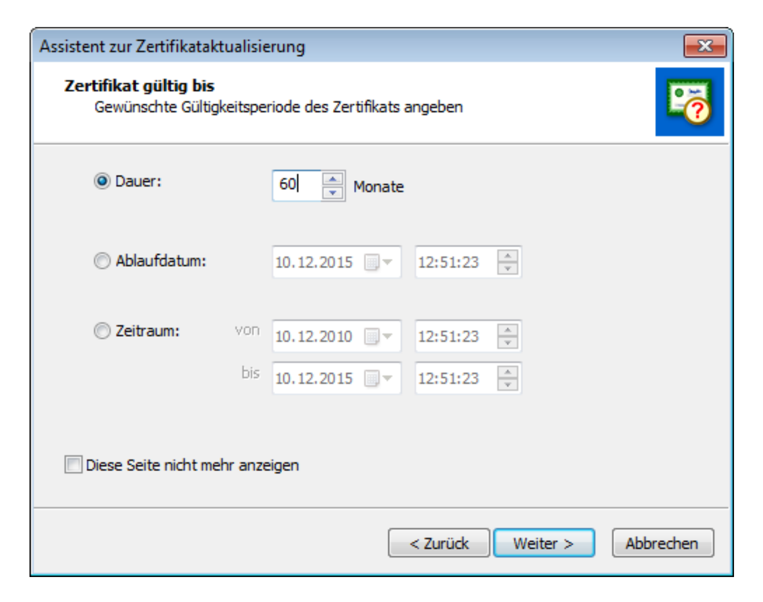


Abbildung 61. Gewünschte Gültigkeitsdauer des Zertifikates angeben

5 Auf der Seite **Ein Zertifikat kann jetzt beantragt werden**:

- Vergewissern Sie sich, dass die Parameter auf den vorherigen Seiten des Assistenten richtig eingegeben wurden. Gehen Sie ggf. mit der Schaltfläche **Zurück** auf die entsprechende Seite des Assistenten und wählen Sie andere Parameter aus.
- Muss die Anfrage mit dem für diese Arbeitsstation aktuellen Drucker ausgedruckt werden, vergewissern Sie sich, dass das Kontrollkästchen **Antragsdaten ausdrücken** aktiviert ist. Anderenfalls deaktivieren Sie das Kontrollkästchen.

Anschließend betätigen Sie die Schaltfläche **Weiter**.

6 Führen Sie im Fenster **Digitales Roulette** (s. Abbildung auf S. 122) vorgeschlagenen Aktionen durch.



Hinweis. Sollte das digitale Roulette in der laufenden Sitzung nicht aktiviert sein, erscheint dieses Fenster nicht.

---

7 Auf der Seite **Assistent wird beendet** klicken Sie auf **Fertig**.

Die Anfrage auf Zertifikatsaktualisierung wird an das Programm ViPNet Key and Certification Authority weitergeleitet.



Hinweis. Die Wartezeit auf die Antwort des Programms ViPNet Key and Certification Authority kann in Abhängigkeit von den Einstellungen dieses Programms variieren. Wenn im Programm ViPNet Key and Certification Authority die automatische Verarbeitung der Zertifikatsanfragen konfiguriert wurde, dann beträgt die Wartezeit selten mehr als 5 Minuten. Wenn die Verarbeitung der Zertifikatsanfragen im Programm ViPNet Key and Certification Authority manuell durchgeführt wird, dann ist die Wartezeit auf eine Antwort nicht begrenzt.

Wenn die Anfrage auf eine Zertifikatsaktualisierung im Programm ViPNet Key and Certification Authority erfüllt wird, dann erhält der betroffene Netzwerkknoten das aktualisierte Zertifikat. Das herausgegebene Zertifikat wird dann sofort nach dem Empfang initialisiert und als aktuelles Zertifikat festgelegt, falls:

- im Fenster **Sicherheitseinstellungen** in der Registerkarte **Signatur** das Kontrollkästchen **Zertifikate, die auf Benutzeranfrage ausgestellt wurden, automatisch initialisieren** aktiviert ist;
- der Container, der den zum Zertifikat passenden privaten Schlüssel enthält, zugänglich ist.



Achtung! Wenn sich der Container mit dem privaten Schlüssel in einem Ordner auf der Festplatte befindet, dann ist er immer verfügbar. Wenn sich der Container auf einem externen Gerät befindet, dann ist er dann verfügbar, wenn das Gerät angeschlossen und der korrekte PIN-Code eingegeben wurde.

Im Fenster **Zertifikatsmanager** wird für die Anfrage, die zum Ausstellen des Zertifikats geführt hat, der Status **Zertifikat wurde initialisiert** (s. Zertifikatsanfrage anzeigen auf S. 152) angezeigt.

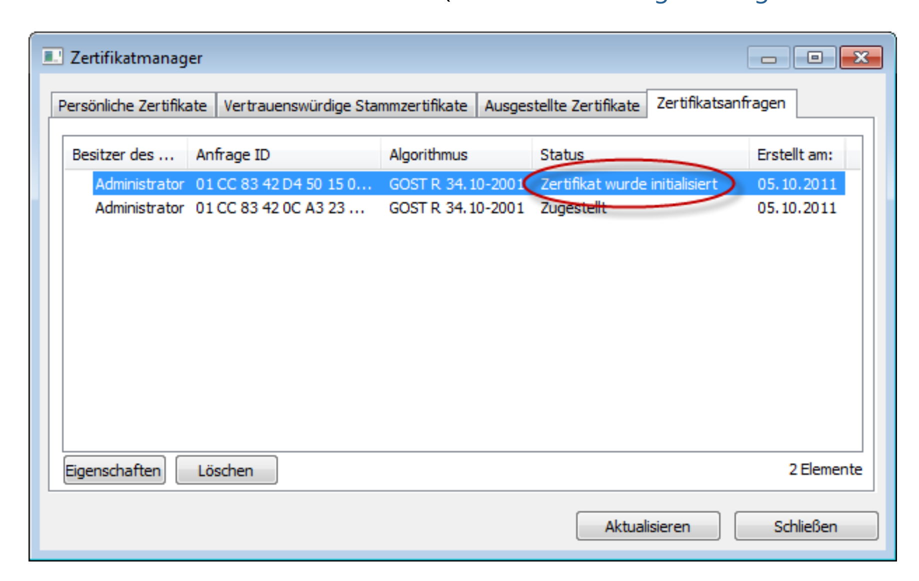


Abbildung 62. Anfragestatus bei Initialisierung des Zertifikats

Wenn ein Zertifikat empfangen, jedoch nicht automatisch initialisiert wurde, dann wird für seine Anfrage der Status **akzeptiert** angezeigt. Führen Sie in diesem Fall die Initialisierung manuell (s. Zertifikate manuell initialisieren auf S. 151) durch.

Wenn eine Anfrage auf Zertifikatsaktualisierung im Programm ViPNet Key and Certification Authority abgelehnt wurde, dann wird kein Zertifikat ausgestellt. Die Zertifikatsanfrage besitzt dann den Status **abgelehnt**. Wenden Sie sich an den Administrator des Programms ViPNet Key and Certification Authority, um den Grund für die Ablehnung zu erfahren.

Das aktualisierte und initialisierte Zertifikat wird in der Liste der privaten Zertifikate des Benutzers (s. Persönliche Benutzerzertifikate anzeigen auf S. 130) angezeigt.

Zertifikat initialisieren

Um ein Zertifikat zu verwenden, das vom ViPNet Key and Certification Authority übermittelt wurde, sollte dieses Zertifikat zunächst initialisiert werden. Das heißt, das Zertifikat sollte durch Zuordnung eines entsprechenden privaten Schlüssels im Container installiert werden.

Zertifikate automatisch initialisieren

Zur automatischen Initialisierung der Zertifikate, die vom Programm ViPNet Key and Certification Authority erhalten wurden, vergewissern Sie sich, dass die Kontrollkästchen **Zertifikate automatisch initialisieren** und **Zertifikate, die auf Initiative des Administrators des Zertifizierungsstelle ausgestellt wurden, automatisch initialisieren** in der Registerkarte **Signatur** des Fensters **Sicherheitseinstellungen** aktiviert sind.

Nach der Aktivierung dieser Kontrollkästchen werden die Zertifikate innerhalb einer Stunde ab dem Empfangszeitpunkt automatisch initialisiert. Zertifikate, die auf Anfrage ausgestellt wurden, können nur dann automatisch initialisiert werden, wenn die Container mit den entsprechenden privaten Schlüsseln verfügbar sind. Anderenfalls können diese Zertifikate ausschließlich manuell (s. Zertifikate manuell initialisieren auf S. 151) initialisiert werden.



Achtung! Wenn sich der Container mit dem privaten Schlüssel in einem Ordner auf der Festplatte befindet, dann ist er immer verfügbar. Wenn sich der Container auf einem externen Gerät befindet, dann ist er dann verfügbar, wenn das Gerät angeschlossen und der korrekte PIN-Code eingegeben wurde.

Wenn ein Zertifikat, das auf Initiative des Administrators des Programms ViPNet Key and Certification Authority ausgestellt wurde, initialisiert wurde, wird das Fenster **Warnung des Sicherheitsdienstes** mit entsprechender Meldung eingeblendet.

Zertifikate manuell initialisieren

Die manuelle Initialisierung der Zertifikate, die vom Programm ViPNet Key and Certification Authority versendet wurden, ist in folgenden Fällen erforderlich:

- Wenn die Kontrollkästchen, die das automatische Initialisieren der Zertifikate ermöglichen , nicht aktiviert wurden;
- Wenn bei einer automatischen Initialisierung des Zertifikats der Container mit dem passenden privaten Schlüssel nicht zugänglich war.

Führen Sie die folgenden Schritte aus, um das erhaltene Zertifikat manuell zu initialisieren:

1. Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur** und klicken Sie auf die Schaltfläche **Ausgestellte Zertifikate**.
2. Wählen Sie im Fenster **Zertifikatmanager** in der Registerkarte **Ausgestellte Zertifikate** das erhaltene Zertifikat, das initialisiert werden soll, und klicken Sie anschließend auf **Initialisieren**.

Das initialisierte Zertifikat wird im Fenster **Zertifikatmanager** in der Registerkarte **Persönliche Zertifikate** angezeigt. Wenn dieses Zertifikat zum Signieren elektronischer Dokumente verwendet werden soll, muss es als aktuelles Zertifikat festgelegt werden (s. Laufendes Zertifikat wechseln auf S. 143).

Arbeiten mit Zertifikatsanfragen

Arbeit mit Zertifikatsanfragen (s. Zertifikatsanfrage auf S. 180) erfolgt im **Zertifikatsmanager** Fenster in der Registerkarte **Zertifikatsanfragen**.

Um das **Zertifikatsmanager** Fenster anzeigen zu lassen:

1 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Signatur**.

2 Betätigen die Schaltfläche **Zertifikatsanfragen**.

Zertifikatsanfrage anzeigen

Um detaillierte Information über die Zertifikatsanfrage (auf S. 180) anzeigen zu lassen:

1 Wählen Sie im Fenster **Zertifikatmanager** in der Registerkarte **Zertifikatsanfragen** die gewünschte Anfrage aus und betätigen Sie danach die Schaltfläche **Eigenschaften** oder doppelklicken Sie auf diese Anfrage.

2 Im Fenster **Zertifikatsanfrage** sehen Sie die gewünschten Informationen in den entsprechenden Registerkarten.

Ggf. kann die Anfrage (mit dem Drucker, der bei dieser Arbeitsstation standardmäßig verwendet wird) mit Hilfe der Schaltfläche **Drucken** ausgedruckt oder über die Schaltfläche **Kopieren nach** in eine Datei des Formates `*.txt` kopiert werden.

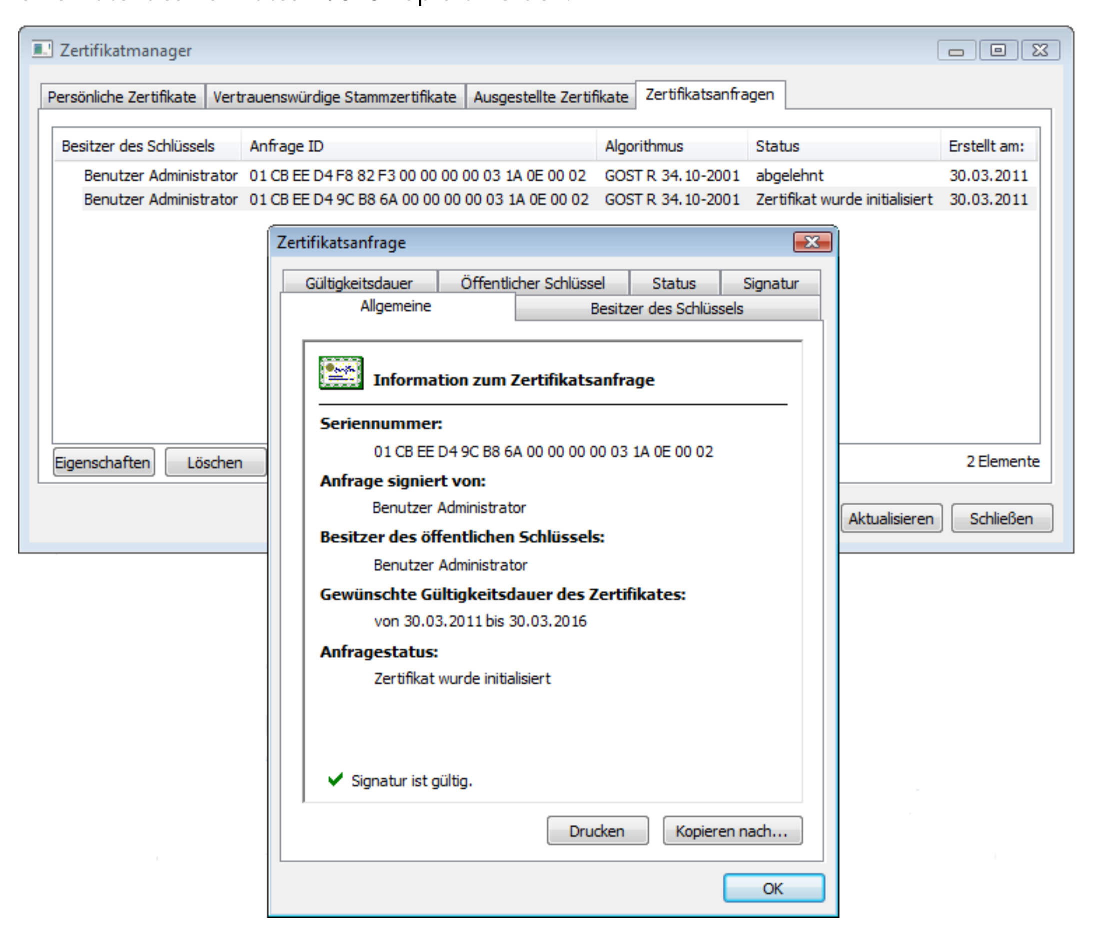


Abbildung 63: Detaillierte Information über die Zertifikatsanfrage anzeigen

Zertifikatsanfrage löschen

Um die Anfrage auf das Zertifikat zu löschen:

1. Wählen Sie im Fenster **Zertifikatmanager** in der Registerkarte **Zertifikatsanfragen** die gewünschte Anfrage (oder mehrere, indem die **Strg**-Taste gedrückt gehalten wird) und klicken danach auf **Löschen**.
2. Klicken Sie im Bestätigungsfenster auf **Ja**.

Eine gelöschte Anfrage wird nicht in der Registerkarte **Zertifikatsanfragen** angezeigt.

Zertifikat exportieren

Im Programm ViPNet kann das Benutzerzertifikat in unterschiedlichen Formaten exportiert werden. Die Wahl des Exportformats hängt von den Zielen ab, die durch den Export erreicht werden sollen.

Der Export des Zertifikats kann für die Erfüllung folgender Aufgaben erforderlich sein:

- Archivierung der Zertifikate;
- Kopieren der Zertifikate für den Gebrauch auf einem anderen Computer;
- Versand der Zertifikate an andere Benutzer, um den Austausch verschlüsselter Nachrichten zu ermöglichen;
- Druck von Zertifikaten.

Um das Zertifikat in eine Datei eines bestimmten Formats zu exportieren:

1 Rufen Sie das Fenster **Zertifikat** für das Zertifikat auf, welches exportiert werden soll (s. Zertifikate anzeigen auf S. 129).

2 Öffnen Sie die Registerkarte **Eigenschaften** und betätigen Sie anschließend die Schaltfläche **Kopieren nach**.

3 Klicken Sie auf der Anfangsseite des Zertifikatexport-Assistenten auf die Schaltfläche **Weiter**.



Tipp. Sollten beim späteren Aufruf des Assistenten Seiten übersprungen werden, ist es zweckmäßig, diese mit den Kontrollkästchen **Diese Meldung nicht mehr anzeigen** zu versehen.

4 Wählen Sie auf der Seite **Format der Exportdatei** eines der angebotenen Formate aus (s. Exportformate für Zertifikate auf S. 155) und betätigen Sie anschließend die Schaltfläche **Weiter**.

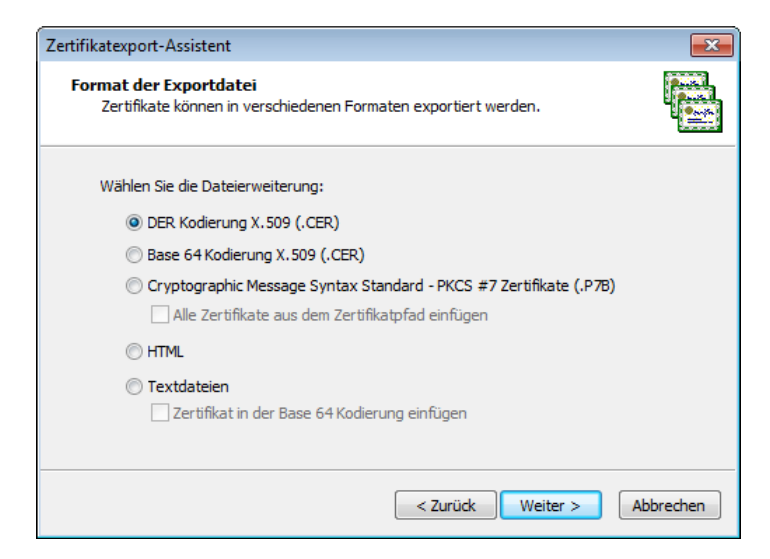


Abbildung 64. Dateiformat auswählen

5 Geben Sie auf der Seite **Name der Exportdatei** den vollständigen Pfad zu der zu erstellenden Datei an und betätigen Sie anschließend die Schaltfläche **Weiter**.

6 Kontrollieren Sie auf der Seite **Zertifikatexport-Assistent beenden**, dass alle auf den vorherigen Seiten angegebenen Exportparameter richtig eingegeben sind, und klicken anschließend auf **Fertig stellen**.

7 Klicken Sie im Fenster mit der Meldung über den erfolgreichen Export auf **OK**.

Exportformate für Zertifikate

Bei der Wahl des Exportformats sollten Sie sich an folgende Richtlinien halten:

- Wenn der Export mit dem Zweck eines späteren Imports auf einen Computer mit dem Betriebssystem Windows erfolgt, sollte bevorzugt das Exportformat PKCS #7 gewählt werden, in erster Linie, weil dieses Format die Beibehaltung der Kette von Zertifizierungsstellen oder des Zertifizierungspfads für jedes Zertifikat ermöglicht. Einige Anwendungen erfordern beim Import des Zertifikats aus einer Datei das Format DER oder Base64. Deswegen sollte das Exportformat in Übereinstimmung mit den Anforderungen der jeweiligen Anwendung oder des Systems, in welchem das Zertifikat voraussichtlich importiert werden soll, gewählt werden.
- Zum Anzeigen und Drucken von Zertifikaten werden das Text- und das HTML-Format benutzt.

Nachfolgend finden Sie detaillierte Informationen über jedes der Exportformate für Zertifikate, die von ViPNet Software unterstützt werden.

- **Cryptographic Message Syntax Standard (PKCS #7)**

  Das PKCS #7-Format ermöglicht die Übertragung eines Zertifikats und aller Zertifikate im Zertifizierungspfad von einem Computer zu einem anderen oder von einem Computer auf externe Datenträger. PKCS #7-Dateien haben normalerweise die Erweiterung *.p7b und sind mit dem ITU-T X.509-Standard kompatibel. PKCS #7 erlaubt Attribute wie Gegensignaturen, die mit gewöhnlichen Signaturen verbunden sind. Attribute wie Signaturzeitpunkt können zusammen mit dem Nachrichteninhalt authentifiziert werden. Weitere Informationen zu PKCS #7 finden Sie auf der PKCS #7-Seite auf der RSA Labs-Website http://www.rsa.com/rsalabs/node.asp?id=2129.

- **Dateien in DER-Codierung X.509**

  DER (Distinguished Encoding Rules) für ASN.1, die in der ITU-T-Empfehlung X.509 definiert sind, bilden einen eingeschränkteren Codierungsstandard als BER (Basic Encoding Rules) für ASN.1. BER sind in der ITU-T-Empfehlung X.209 definiert, auf der DER basiert. BER und DER bieten eine plattformunabhängige Methode für das Codieren von Objekten, beispielsweise Zertifikaten und Nachrichten, für die Übertragung zwischen Geräten und Anwendungen.

  Während der Zertifikatcodierung verwenden die meisten Anwendungen DER, da das Zertifikat (die Zertifikatanforderungsinformationen) DER-codiert und signiert sein muss. DER-Zertifikatdateien haben die Erweiterung .cer.

  Weitere Informationen finden Sie im Dokument "ITU-T Recommendation X.509, Information Technology - Open Systems Interconnection -The Directory: Authentication Framework" auf der International Telecommunication Union (ITU)-Website http://www.itu.int/en/Pages/default.aspx.

- **Dateien in Base64-Codierung X.509**

  Dies ist eine Codierungsmethode, die für die Verwendung mit dem Protokoll S/MIME entwickelt wurde, einem gängigen Standardverfahren für die Übertragung binärer Dateien über das Internet. Mithilfe von Base64 werden Dateien im ASCII-Textformat codiert, wodurch die Dateien beim Passieren von Gateways praktisch nicht beschädigt werden. Das Protokoll S/MIME gewährleistet den Betrieb einiger Verschlüsselungsdienste für Messaging-Anwendungen, inklusive der Sicherstellung der Nichtabstreitbarkeit (durch digitale Signaturen), der Vertraulichkeit und der Datensicherheit (durch Verschlüsselung, Authentifizierung und Nachrichtenintegrität). Base64-Zertifikatdateien haben die Erweiterung .cer.

In der MIME-Spezifikation (Multipurpose Internet Mail Extensions), RFC 1341 und folgende, ist ein Verfahren für das Codieren beliebiger binärer Informationen für die Übertragung per E-Mail definiert.

Weitere Informationen finden Sie im Dokument „RFC 2633 S/MIME Version 3 Message Specification, 1999“ auf der Internet Engineering Task Force (IETF)-Website http://www.ietf.org/rfc/rfc2633.txt?number=2633.

- **Dateien im HTML-Format**

  Dateien für Druck und Anzeige in jedem Webbrowser, sowie in Office-Programmen und anderen Anwendungen, die die Auszeichnungssprache HTML unterstützen.

- **Textdateien**

  ANSI-codierte Dateien für die Anzeige in jedem Texteditor und für den Druck.

Arbeiten mit dem Schlüsselcontainer

Der Schlüsselcontainer enthält den privaten Signaturschlüssel (s. Privater Schlüssel auf S. 179) und das Zertifikat (auf S. 180), das dem privaten Schlüssel entspricht.

Im Programm ViPNet Business Mail sind folgende Operationen mit dem Schlüsselcontainer verfügbar:

- Installation (s. Schlüsselcontainer installieren auf S. 162).

  Die Installation eines neuen Containers oder ein Wechsel des Schlüsselcontainers des aktuellen Zertifikats kann in folgenden Fällen erforderlich werden:

  - Wenn dem Zertifikat kein entsprechender privater Schlüssel, der in einem Schlüsselcontainer gespeichert ist, zugeordnet wurde, weil zum Beispiel das Zertifikat getrennt vom privaten Schlüssel aufbewahrt wird. Der Schlüsselcontainer kann sowohl zusammen mit dem Zertifikat (s. Zertifikate im Speicher installieren auf S. 135), als auch gesondert installiert werden (s. Schlüsselcontainer installieren auf S. 162) (z.B. wenn der private Schlüssel im Container aufbewahrt wird und das Zertifikat auf Anfrage des Benutzers im Programm ViPNet Key and Certification Authority erstellt wurde).
  - Wenn der Container von einer anderen Anwendung erstellt oder von einem anderen Rechner übertragen wurde.

- Gespeichertes Containerpasswort ändern oder löschen (s. Schlüsselcontainerpasswort ändern auf S. 159).

  Es wird empfohlen, das angegebene Passwort für den Schlüsselcontainer maximal ein Jahr lang zu benutzen. Nach Ablauf dieser Frist sollte ein neues Passwort festgesetzt werden. Das Löschen des gespeicherten Passworts für den Schlüsselcontainer kann dann erforderlich sein, wenn sich die Nutzungsbedingungen für das Passwort und (oder) die Richtlinien Ihrer Organisation geändert haben, wodurch das Speichern von Passwörtern auf dem Rechner nicht mehr erlaubt ist.

- Änderung des Containerortes (s. Schlüsselcontainer übertragen auf S. 163).

  Der aktuelle Schlüsselcontainer muss in folgenden Fällen verlegt werden:

  - wenn der Standort des Containers geändert werden soll, da zum Beispiel der bisherige Speicherort des Containers als unsicher eingestuft wurde;
  - beim Wechsel des Authentisierungsmodus auf **PIN und Authentisierungsgerät**, falls die Signatur- und Verschlüsselungsvorgänge innerhalb von Drittanwendungen stattfinden, und der Container dabei ursprünglich nicht auf einem externen Gerät für die Authentifizierung gespeichert war.



Achtung! Im Rahmen des Netzwerks auf Basis der Software ViPNet Administrator kann der Schlüsselcontainer nur von einem Benutzer mit Signaturberechtigung bearbeitet werden. Diese Berechtigung haben nur die Benutzer des ViPNet Netzwerkes im Programm ViPNet Network Control Center.

Um mit dem Schlüsselcontainer zu arbeiten:

1 Öffnen Sie die Registerkarte **Schlüssel**.

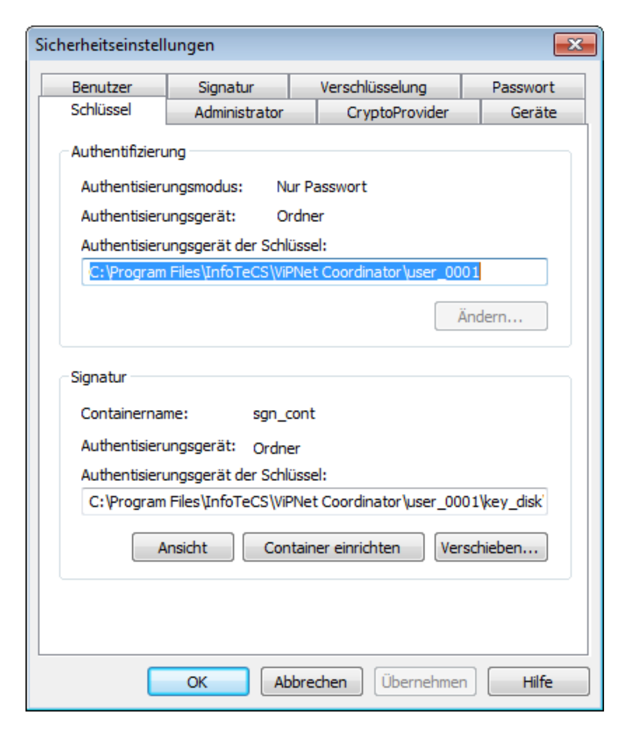


Abbildung 65. Arbeiten mit Container mit privatem Schlüssel

2 Betätigen Sie in der Gruppe **Signatur** eine der folgenden Schaltflächen:

- **Ansicht**, d.h. um nähere Information über den verwendeten Container zu bekommen sowie die Containereigenschaften zu ändern:
  - Passwort ändern (s. Schlüsselcontainerpasswort ändern auf S. 159);
  - Passwort löschen (s. Passwort für Schlüsselcontainer löschen, der auf dem Computer gespeichert ist auf S. 161);
  - Konformitätsprüfung des privaten Schlüssels mit dem Zertifikat (s. Schlüsselcontainer prüfen auf S. 161);
  - Privaten Schlüssel löschen.
- **Container einrichten**, d.h. um einen neuen Container zu installieren und den laufenden Container zu wechseln (s. Schlüsselcontainer installieren auf S. 162).
- **Verschieben**, d.h. um den Pfad zum Container zu ändern.



Hinweis. In Gruppe **Signatur** werden Informationen über den privaten Schlüssel angezeigt, der dem aktuell verwendeten Zertifikat zugeordnet ist. Bei Installation eines neuen Schlüsselcontainers (s. Schlüsselcontainer installieren auf S. 162) ändern sich die in der Registerkarte **Signatur** angezeigten Informationen über das laufende Zertifikat automatisch.

Schlüsselcontainerpasswort ändern

Es wird empfohlen, das angegebene Passwort für den Schlüsselcontainer maximal ein Jahr lang zu benutzen. Nach Ablauf dieser Frist sollte ein neues Passwort festgesetzt werden.

Zum Ändern des Containerpassworts:

1 Klicken Sie im Fenster **Sicherheitseinstellungen** in der Registerkarte **Schlüssel** (s. Abbildung auf S. 158) auf **Anzeigen**.

2 Klicken Sie Im Fenster **Schlüsselcontainereigenschaften** auf **Passwort ändern**.

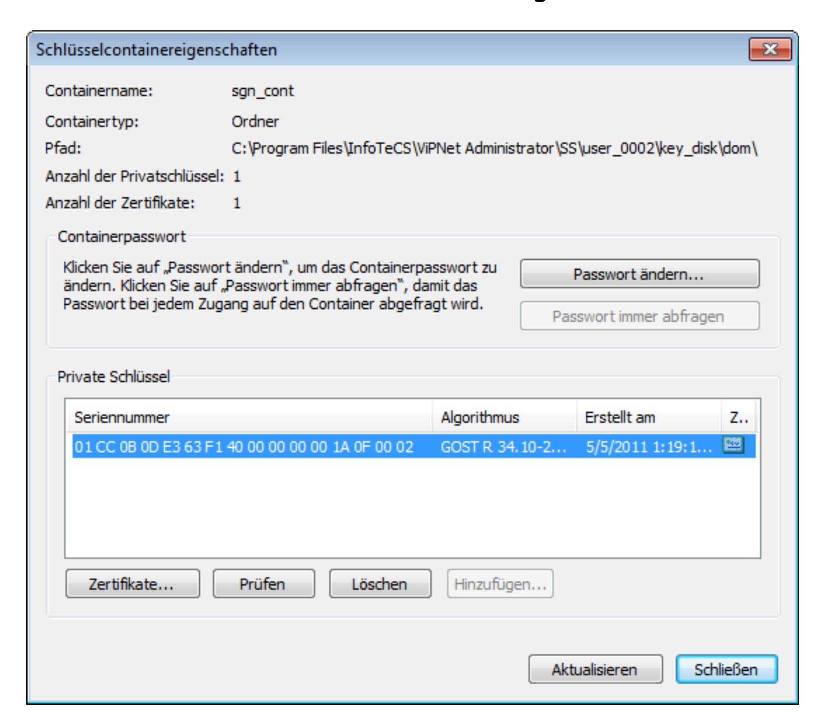


Abbildung 66. Fenster „Schlüsselcontainereigenschaften"

3 Beim Einblenden der Meldung „Für diesen Container kann das Passwort nur in den Sicherheitseinstellungen der ViPNet Software geändert werden" klicken Sie auf **OK**, schließen Sie das Fenster **Containereigenschaften** und ändern Sie danach das Benutzerpasswort (s. Ändern des Benutzerpassworts auf S. 120).

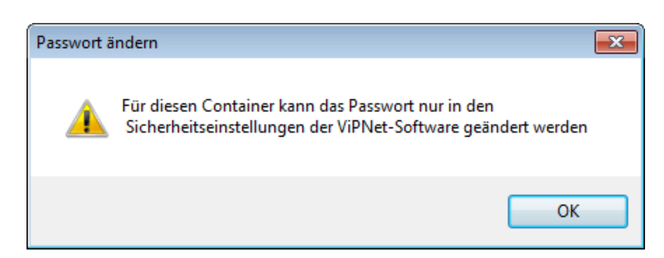


Abbildung 67. Meldung, dass die Passwortänderung nicht möglich ist



Hinweis. Dieses Dialogfeld erscheint, weil der Schlüsselcontainer nicht mit dem Passwort sondern mit dem Benutzerschlüssel geschützt ist. In diesem Fall stimmt das Containerpasswort mit dem Benutzerpasswort überein, deswegen kann das Containerpasswort nur zusammen mit dem Benutzerpasswort geändert werden.

4 Wenn der Schlüsselcontainer des ViPNet Benutzers im Programm ViPNet Registration Point erstellt oder aus dem Benutzerschlüsselordner (standardmäßig `C:\Program Files (x86)\InfoTeCS\<Name der installierten Software ViPNet>\user_<Benutzer-Id>\key_disk\dom`) in einen anderen Ordner übertragen wurde (s. Schlüsselcontainer übertragen auf S. 163), wird nach dem Anklicken der Schaltfläche **Passwort ändern** das Fenster **Passwort** eingeblendet.

5 Im Fenster **Passwort** geben Sie das aktuelle Passwort für den Zugang zum Container ein und klicken auf die Schaltfläche **OK**.



Hinweis. War vorher der Modus **Passwort speichern** aktiv, erscheint das Fenster **Passwort** nicht.

6 Geben Sie im Fenster **ViPNet CSP - Passwort des Schlüsselcontainers** das neue Passwort in den Feldern **Passwort eingeben** und **Passwort** ein. Klicken Sie auf **OK**.



Abbildung 68. Passwort für den Zugriff auf den Container ändern



Achtung! Es darf kein Passwort mit einer Länge von 32 Symbolen erstellt werden. Passwörter dieser Länge können in den laufenden Versionen der ViPNet Anwendungen nicht verwendet werden. Diese Einschränkung ist bedingt durch den bestehenden Algorithmus zur Weiterleitung des Passworts an den Cryptoprovider. In Übereinstimmung mit diesem Algorithmus darf die Länge des Passworts nicht mehr als 31 Zeichen betragen.

Das Passwort für den Zugang auf den Container ist geändert.

Passwort für Schlüsselcontainer löschen, der auf dem Computer gespeichert ist

Das Löschen des gespeicherten Passworts für den Schlüsselcontainer kann dann erforderlich sein, wenn sich die Nutzungsbedingungen für das Passwort und (oder) die Richtlinien Ihrer Organisation geändert haben, wodurch das Speichern von Passwörtern auf dem Rechner nicht mehr erlaubt ist.

Um ein gespeichertes Passwort für den Zugang auf den Container zu löschen und das Eingabefeld für das Passwort anzuzeigen:

1. Klicken Sie im Fenster **Sicherheitseinstellungen** in der Registerkarte **Schlüssel** (s. Abbildung auf S. 158) auf **Ansicht**.
2. Klicken Sie im Fenster **Containereigenschaften** (s. Abbildung auf S. 159) auf **Passwort immer abfragen**.

Das gespeicherte Passwort ist gelöscht. Nun muss das Passwort jedes Mal beim Zugriff auf den Schlüsselcontainer eingegeben werden.

Schlüsselcontainer prüfen

Eine Überprüfung des Containers führt zur Feststellung, dass die Containerdatei nicht beschädigt ist, und dass die im Container gespeicherten Zertifikat und privater Schlüssel miteinander übereinstimmen und für die Arbeit mit geschützten Dokumenten verwendet werden können.

Um zu prüfen, ob der private Schlüssel und das Zertifikat, die im Container enthalten sind, einander entsprechen:

1. Wählen Sie im Fenster **Schlüssselcontainereigenschaften** (s. Abbildung auf S. 159) in der Liste **Private Schlüssel** die Zeile des privaten Schlüssels aus.
2. Klicken Sie auf **Prüfen**.
3. Geben Sie im Fenster **ViPNet CSP - Passwort des Schlüsselcontainers** das Containerpasswort ein und betätigen Sie mit **OK**.

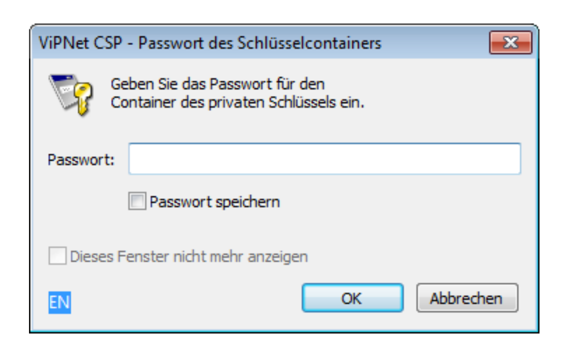


Abbildung 69. Passwort für den Container des privaten Schlüssels eingeben

4 Danach wird ein Datenfragment erstellt, welches mit dem privaten Schlüssel signiert wird, wonach die digitale Signatur mit dem Zertifikat des öffentlichen Schlüssels geprüft wird. Somit wird der private Schlüssel auf seine Tauglichkeit und seine Übereinstimmung mit dem im Container enthaltenen Zertifikat geprüft.



Hinweis. Die Prüfung ist erst dann möglich, wenn der Container das Zertifikat enthält, welches diesem privaten Schlüssel entspricht. Das Zertifikat darf im Schlüsselcontainer fehlen, falls es vom Container getrennt aufbewahrt wird. Das Zertifikat wird getrennt vom Schlüsselcontainer aufbewahrt, wenn die Zertifikatsanfrage im Programm ViPNet CSP erstellt wurde. Wenn die Anfrage in einem anderen Programm erzeugt wurde, dann wird das Zertifikat automatisch im Schlüsselcontainer abgelegt.

Bei der Prüfung des privaten Schlüssels wird die Prüfung der Gültigkeit des Zertifikats (seine Laufzeit, sein Vorhandensein in den Listen der abgerufenen Zertifikate usw.) nicht durchgeführt.

Ist die Prüfung des privaten Schlüssels erfolgreich, wird die Meldung „Zertifikat wurde erfolgreich geprüft" angezeigt.

Schlüsselcontainer installieren

Die Installation eines neuen Schlüsselcontainers oder der Wechsel des Schlüsselcontainers des aktuellen Zertifikats kann in folgenden Fällen erforderlich werden:

- wenn bei der Installation des Zertifikats im Zertifikatspeicher des Systems oder im Zertifikatspeicher des Programms ViPNet Business Mail (s. Zertifikate im Speicher installieren auf S. 135) dem Zertifikat kein entsprechender Schlüsselcontainer zugeordnet wurde, weil zum Beispiel das Zertifikat getrennt vom privaten Schlüssel aufbewahrt wird und dementsprechend nicht im Schlüsselcontainer enthalten ist;
- wenn der Schlüsselcontainer von einer anderen Anwendung erstellt oder von einem anderen Rechner übertragen wurde.



Hinweis. Es können nur Schlüsselcontainer installiert oder ausgetauscht werden, die in ViPNet Software der Version 3.2.x oder höher erstellt wurden.

Um einen neuen Container zu installieren oder den aktuellen Container zu wechseln:

1 Klicken Sie im Fenster **Sicherheitseinstellungen** in der Registerkarte **Schlüssel** (s. Abbildung auf S. 158) auf **Container einrichten**.

2 Geben Sie im Fenster **Initialisierung des Schlüsselcontainers** den Speicherort des Containers mit dem privaten Schlüssel an:

   - Ordner auf der Festplatte,
   - Gerät mit Angabe seiner Parameter und des PIN-Codes.

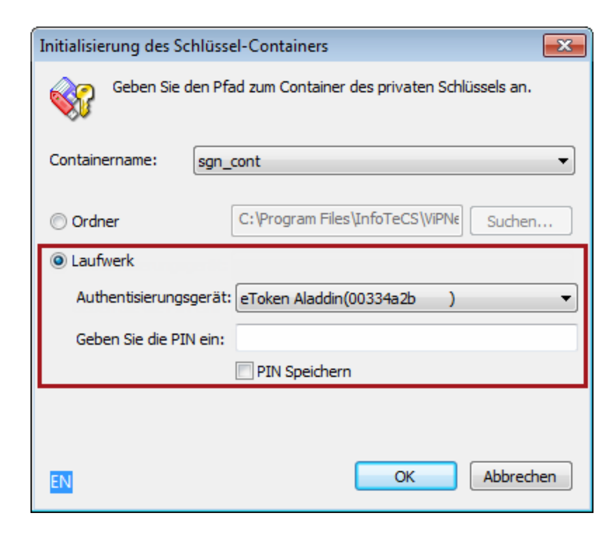


Abbildung 70. Container von externem Gerät aus initialisieren

Klicken Sie auf **OK**.

3 Kilcken Sie im Fenster **Zertifikat auswählen** auf **OK**.

Dadurch werden der private Schlüssel und das Zertifikat, die im ausgewählten Container gespeichert sind, als aktuell festgelegt. Informationen über das Zertifikat, das im installierten Container enthalten ist, werden in der Registerkarte **Signatur** angezeigt.

Schlüsselcontainer übertragen

Die Übertragung des aktuellen Schlüsselcontainers kann dann erforderlich sein, wenn der Standort des Containers geändert werden soll, da z. B. der alte Containerstandort als nicht sicher genug eingestuft wurde.



Hinweis. Es können nur Schlüsselcontainer übertragen werden, die in ViPNet Software der Version 3.2.x oder höher erstellt wurden.

Die Übertragung des Schlüsselcontainers auf Geräte mit Hardware-basierten kryptographischen Funktionen wird nicht unterstützt.

Um den Speicherort des Containers zu ändern:

1 Klicken Sie im Fenster **Sicherheitseinstellungen** in der Registerkarte **Schlüssel** (s. Abbildung auf S. 158) auf **Verschieben**.

2 Geben Sie im Fenster **Initialisierung des Containers des Schlüssels** den neuen Speicherort des Schlüsselcontainer an:

- Ordner auf der Festplatte,
- Gerät mit Angabe seiner Parameter und des PIN-Codes.



Hinweis. Um ein externes Gerät verwenden zu können, müssen der Treiber dieses Gerätes installiert sein. Die Übersicht über die verfügbaren Datenträger sowie nützliche Information zu deren Verwendung ist im Bereich Externe Datenträger (auf S. 174).

Der Schlüsselcontainer wird gemäß dem angegebenen Pfad übertragen.

Installation des Zertifikats im Schlüsselcontainer

Wenn sich aus irgendwelchen Gründen kein Zertifikat im Schlüsselcontainer befindet (z. B. wenn Sie das Zertifikat im Zuge der Zertifikatinstallation im Speicher (s. Zertifikate im Speicher installieren auf S. 135) nicht mit dem privaten Schlüssel abgeglichen haben), dann sollte das Zertifikat manuell in den Container installiert werden. Das Zertifikat kann sowohl im Programm ViPNet CSP als auch im Fenster **Sicherheitseinstellungen** in den Container installiert werden. In beiden Fällen sollte der Schlüsselcontainer im Programm installiert werden.

Die Installation des Zertifikats im Container mit Hilfe des Programms ViPNet CSP wird im Handbuch „ViPNet CSP. Benutzerhandbuch" beschrieben. Wenn Sie das Zertifikat in den Schlüsselcontainer über das Fenster **Sicherheitseinstellungen** installieren möchten, dann führen Sie die folgenden Schritte aus:

1 Wechseln Sie zur Registerkarte **Schlüssel** (s. Abbildung auf S. 158).

2 Installieren Sie den Schlüsselcontainer, falls er noch nicht installiert ist (s. Schlüsselcontainer installieren auf S. 162).

3 Öffnen Sie die Containereigenschaften mit Hilfe der Schaltfläche **Ansicht**.

4 Klicken Sie im Fenster **Schlüsselcontainereigenschaften** auf die Schaltfläche **Hinzufügen**.

5 Geben Sie im eingeblendeten Fenster die Zertifikatsdatei an, die dem privaten Schlüssel im Container entspricht. Sobald das Programm feststellt, dass das gewählte Zertifikat dem privaten Schlüssel entspricht, wird das Zertifikat dem Container hinzugefügt. Anderenfalls wird eine entsprechende Meldung angezeigt.



Mögliche Störungen und entsprechende Gegenmaßnahmen

Authentifizierung mittels Zertifikat kann nicht durchgeführt werden

Wenn Sie sich in einem ViPNet-Programm nicht anmelden können und dabei für die Authentifizierung ein Zertifikat und den entsprechenden privaten Schlüssel verwenden, die beide auf einem externen Gerät gespeichert sind, dann kann dieses Problem folgende Ursachen haben:

- Das Zertifikat entspricht dem RSA-Standard nicht.
- Das externe Datenspeichergerät unterstützt nicht den Standard PKCS#11. Anhand der Informationen im Abschnitt Externe Datenträger (auf S. 174) können Sie überprüfen, ob Ihr Gerät diesen Standard unterstützt.
- Die Gültigkeitsdauer des gewählten Zertifikats ist abgelaufen. Bei Auswahl eines abgelaufenen Zertifikats wird eine entsprechende Meldung angezeigt. In diesem Fall sollten Sie das Zertifikat an den Administrator Ihrer Zertifizierungsstelle zur Aktualisierung weiterleiten.
- Das gewählte Zertifikat ist in der Zertifikatsperrliste des Zertifikatspeichers auf dem aktuellen Knoten enthalten. Bei Auswahl eines widerrufenen Zertifikats wird eine entsprechende Meldung angezeigt. In diesem Fall sollten Sie sich an den Administrator Ihrer Zertifizierungsstelle wenden.

- Der Geltungsbereich des gewählten Zertifikats umfasst nicht die Echtheitsüberprüfung des Clients. Der Geltungsbereich wird im Fenster **Zertifikat** in der Registerkarte **Eigenschaften** im Feld **Erweiterte Schlüsselverwendung** angezeigt. In diesem Fall sollten Sie sich an den Administrator Ihrer Zertifizierungsstelle wenden, damit das Zertifikat neu ausgestellt wird.
- Das Ausstellerzertifikat ist nicht im Systemzertifikatspeicher **Vertrauenswürdige Stammzertifizierungsstelle** installiert. In diesem Fall sollten Sie das Aussteller-Zertifikat beim Administrator Ihrer Zertifizierungsstelle anfordern und im angegebenen Systemzertifikatspeicher installieren. Doppelklicken Sie dazu auf das Zertifikat und folgen Sie dann den Anweisungen des Zertifikat-Installationsassistenten.

Probleme beim Versenden von Nachrichten in Business Mail

Dass eine Nachricht in „Business Mail“ nicht an den Empfänger zugestellt wurde, ist an den folgenden Attributen dieser Nachricht erkennbar:

- : verpackt; die Nachricht ist versandbereit, wurde aber noch nicht an den Kommunikationsserver (Coordinator, auf welchem der gegebene Client im Programm ViPNet Network Control Center registriert ist) weitergeleitet.
- : versendet; die Nachricht wurde an den Routingserver, jedoch nicht an den Netzwerkknoten des Empfängers weitergeleitet.

Nachricht verpackt, aber nicht versendet

Wenn die versendete Nachricht das Symbol besitzt, führen Sie auf dem Client im Programm ViPNet Monitor folgende Schritte aus:

- Überprüfen Sie die Verbindung zum Kommunikationsserver des Clients.



Hinweis. Um den Namen des Kommunikationsserver zu erfahren, öffnen Sie im Programm ViPNet MFTP im Fenster **Einstellungen** die Registerkarte **Kanäle**. Der Kommunikationsserver ist in der ersten Zeile der Liste aufgeführt.

- Prüfen Sie die Informationen in der Logdatei der IP-Pakete.

Verbindung zum Kommunikationsserver überprüfen

Führen Sie im Programm ViPNet Monitor folgende Schritte aus, um die Verbindung zum Coordinator zu überprüfen:

1. Wählen Sie im Bereich **Privates Netzwerk** den Coordinator aus, der als Kommunikationsserver für den gegebenen Client auftritt.
2. Klicken Sie in der Symbolleiste auf **Verbindung** oder drücken Sie die Taste **F5**.
3. Warten Sie, bis im Fenster **Status** in Spalte **Status** die Meldung über die Erreichbarkeit des Coordinators angezeigt wird. Die Überprüfung der Verbindung kann bis zu einer Minute dauern.



Tipp. Führen Sie die Prüfung mehrmals in einem Intervall von 1-2 Minuten durch. Wenn zum Zeitpunkt der Verbindungsüberprüfung auf dem Coordinator eine Aktualisierung der Adresslisten und Schlüssel durchgeführt wird, bleibt der Coordinator innerhalb eines gewissen Zeitraums nicht erreichbar.

Wenn keine Verbindung zum Coordinator besteht (im Fenster **Status** wird für den Coordinator der Wert **Nicht erreichbar** eingeblendet), überprüfen Sie die Einträge in der Logdatei der IP-Pakete.

Daten in Logdatei der IP-Pakete anzeigen

Führen Sie einen der folgenden Schritte aus, um Daten aus der Logdatei der IP-Pakete im Programm ViPNet Monitor anzuzeigen:

- Wählen Sie in der Navigationsleiste den Bereich **Logdatei** und klicken Sie im Ansichtsbereich auf die Schaltfläche **Suche**.
- Klicken Sie im Bereich **Privates Netzwerk** mit der rechten Maustaste auf den Coordinator, der als Routingserver für den gegebenen Client auftritt, und wählen Sie im Kontextmenü den Eintrag **Logdatei**. Klicken Sie anschließend im eingeblendeten Bereich **Logdatei** auf die Schaltfläche **Suche**.

Überprüfen Sie die Informationen über ein- und ausgehende IP-Pakete:

- In der Logdatei der IP-Pakete wurden ausgehende IP-Pakete (,), die für den Coordinator bestimmt sind, möglicherweise nicht registriert.

  Dies kann darauf hinweisen, dass auf dem verwendeten Computer die IP-Adresse des Gateways nicht definiert ist. Um dieses Problem zu lösen, geben Sie in den Netzwerkeinstellungen von Windows die IP-Adresse des Gateways an (**Standardgateway**).

- In der Logdatei der IP-Pakete wurden ausgehende IP-Pakete, die für den Coordinator bestimmt sind, mit Code 40 registriert, eingehende Antwort-IP-Pakete (,) jedoch nicht.

  Führen Sie in diesem Fall auf dem Client in der Kommandozeile den Befehl ping <ip> aus, wobei <ip> – die sichtbare IP-Adresse des Coordinators darstellt.



Hinweis. Die sichtbaren IP-Adressen des Coordinators (in Abhängigkeit von den Einstellungen reell oder virtuell) sind in der Registerkarte **Privates Netzwerk** im Eigenschaften-Fenster des Coordinators in fetter Schrift hervorgehoben.

Wenn nach Durchführung des Befehls ping in der **Logdatei** der IP-Pakete die eingehenden Antwort-IP-Pakete des Coordinators noch immer nicht registriert werden, und im Konsolenfenster die Meldung **Antwortzeit überschritten** (**Request time out**) eingeblendet wird:

- Überprüfen Sie die Routen für die Weiterleitung der Daten vom Client zum Coordinator (zum Beispiel mit Hilfe des Kommandozeilenbefehls route print).
- Stellen Sie sicher, dass in den Windows-Netzwerkeinstellungen auf dem Client die richtige IP-Adresse eingeblendet wird.

- Führen Sie auf dem Coordinator den Befehl `ping` aus, um die Verbindung zum aktuellen Client zu überprüfen.

Wenn nach Ausführung des Befehls `ping` Antworten vom Coordinator empfangen werden, die Nachrichten aber noch immer nicht versendet werden, führen Sie die folgenden Schritte durch:

- Stellen Sie sicher, dass auf dem Coordinator das Programm ViPNet Monitor und das MFTP-Modul gestartet sind.
- Überprüfen Sie, ob in der Logdatei der IP-Pakete die Pakete des MFTP-Moduls registriert werden (in Spalte **Quellport** oder **Zielport** wird für diese Pakete der Wert 5000, 5001 oder 5002 angezeigt). Andernfalls vergewissern Sie sich, dass auf dem verwendeten Computer das MFTP-Modul gestartet ist.
- Stellen Sie sicher, dass in den Einstellungen des Transportmoduls auf dem Client der Verbindungskanal zum Routingserver aktiviert ist. Öffnen Sie dazu im Programm ViPNet MFTP im Fenster **Einstellungen** die Registerkarte **Kanäle**. Stellen Sie sicher, dass im Eintrag des Routingservers (erste Zeile) der Kanaltyp **MFTP** angegeben ist.

- In der Logdatei der IP-Pakete auf dem Client und auf dem Coordinator sind blockierte IP-Pakete mit Ereignisnummer 1 registriert.

  Dies kann damit verbunden sein, dass vom Client kein Schlüsselupdate nach dem Austausch der Masterschlüssel des ViPNet-Netzwerks oder nach einer Kompromittierung (des gegebenen Clients oder des Coordinators) erhalten wurde. Zum Lösen dieses Problems müssen Sie vom Administrator Ihres ViPNet-Netzwerks eine neue Schlüsseldistribution beziehen und anschließend manuell das Schlüsselupdate durchführen.

Nachricht versendet, aber nicht weitergeleitet

Wenn die Nachricht das Symbol besitzt:

1. Stellen Sie sicher, dass der Netzwerkknoten des Empfängers aktiviert ist, und die Programme ViPNet Monitor und ViPNet MFTP auf diesem Knoten gestartet sind.
2. Wenden Sie sich an den Administrator Ihres ViPNet-Netzwerks, um diese Prüfung auf allen Computern durchzuführen, die einen Teil der Route für die Datenübertragung von Ihrem Client zum Empfängerknoten bilden.

Anhang kann nicht verschlüsselt werden

Beim Versuch, eine E-Mail mit Anhang abzusenden, wird die folgende Fehlermeldung eingeblendet: „Die Schlüssel für den Verbindungsaufbau zum Netzwerk <%s> sind veraltet. Diese Schlüssel können nicht dazu benutzt werden, Dateien mit einer Größe von mehr als 4 MB zu verschlüsseln. Wenden Sie sich an den Administrator des ViPNet Netzwerks“.

Der Grund für diesen Fehler besteht darin, dass für Verbindungen zum Netzwerk, dessen Nummer in der Nachricht angegeben ist, Schlüssel im alten Format verwendet werden. Mit Hilfe solcher Schlüssel können

Anhänge mit einer Größe von mehr als 4 MB nicht verschlüsselt werden. Informieren Sie den Administrator Ihres ViPNet Netzwerks über die Notwendigkeit der Aktualisierung des Internetzwerk-Masterschlüssels für das betroffene Netzwerk, um das Problem zu lösen.

Wiederherstellung der Postdatenbank

Allgemeine Informationen

Die Wiederherstellung der Postdatenbank kann im Falle ihrer Beschädigung notwendig werden. Diese Notfallsituation kann in folgenden Fällen auftreten:

- Beim Neustart des Computers (zum Beispiel bei Störungen in der Stromversorgung oder als Folge eines Fehlers im Betriebssystem) während der aktiven Laufzeit des Programms „Business Mail“ (beim Erstellen von Nachrichten, bei Änderungen von Einstellungen und so weiter).
- Beim zwangsweisen Beenden des Programms.
- Bei Verlust oder Beschädigung von zumindest einer Steuerungsdatei des Programms.
- Bei fehlendem Datenzugang als Folge eines Festplattendefekts auf dem verwendeten Rechner.

In der Regel wird die Wiederherstellung der Postdatenbank automatisch durchgeführt und erfordert keine weiteren Schritte seitens des Benutzers. Für eine automatische Wiederherstellung müssen sich im Ordner `\MS` folgende Steuerungsdateien befinden, die nicht beschädigt sein dürfen: `attach3.db`, `rcpt3.db`, `folders3.db`, `docs3.db`. Falls zumindest eine dieser Dateien fehlt oder beschädigt ist, muss die Wiederherstellung der Postdatenbank manuell vorgenommen werden (s. Prozedur zur Wiederherstellung der Postdatenbank auf S. 172).



Hinweis. Der Standort des Ordners \MS hängt von der Zusammenstellung der Programme ab, die auf dem verwendeten Computer installiert sind:

- Falls ViPNet Business Mail installiert ist (als Bestandteil der Software ViPNet Client oder separat), dann befindet sich der Ordner standardmäßig in C:\Program Files\InfoTeCS\ViPNet Client.
- Falls ViPNet Administrator und ViPNet Client installiert sind, dann befindet sich der Ordner standardmäßig in C:\Program Files\InfoTeCS\ViPNet Administrator\SS.

Auf die Notwendigkeit einer manuellen Wiederherstellung der Postdatenbank verweisen die während der Laufzeit des Programms „Business Mail“ eingeblendeten Meldungen, die weiter unten aufgeführt sind.

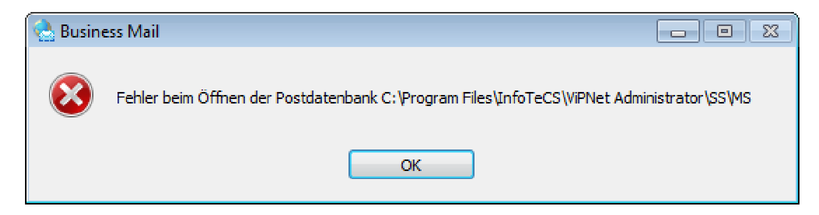


Abbildung 71. Meldung über den Fehler beim Öffnen der Postdatenbank

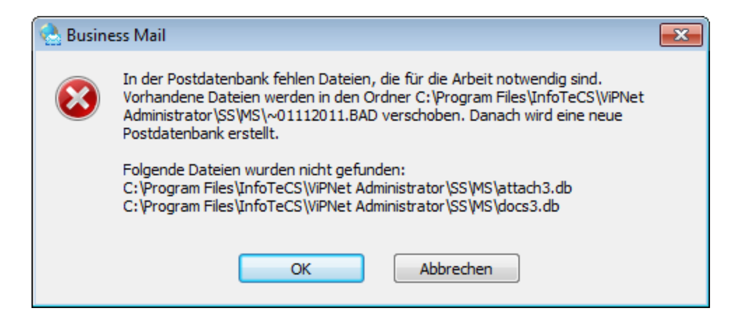


Abbildung 72. Meldung über fehlende Steuerungsdateien



Achtung! Um den Prozess der Wiederherstellung der Postdatenbank einfacher zu gestalten, wird es empfohlen, die Nachrichten des Programms „Business Mail" regelmäßig zu archivieren. Die Archivierung kann automatisch oder mit Hilfe des Befehls **Datei** > **Archivieren** durchgeführt werden. Das Archiv wird im Ordner `\MSArch` abgelegt, der auf dem gleichen Pfad wie der Ordner `\MS` liegt.

Prozedur zur Wiederherstellung der Postdatenbank

Die manuelle Wiederherstellung der Postdatenbank kann auf eine der folgenden Arten durchgeführt werden:

- Mit Hilfe des Ordners mit der Erweiterung REP, der sich im Verzeichnis `\MS` befindet.

  Die Ordner mit der Erweiterung REP werden automatisch bei nicht ordnungsgemäßer Beendigung des Programms erstellt und enthalten Steuerungsdateien mit Daten, die zum Zeitpunkt der Ordnererstellung aktuell waren. Das Erstellungsdatum ist im Namen des Ordners im Format **~ddmmjjjj** enthalten.

- Mit Hilfe des Ordners `\MSArch`, der auf dem gleichen Pfad liegt wie der Ordner `\MS`.

  Der Ordner `\MSArch` wird bei Nachrichtenarchivierung (automatisch oder mit Hilfe des Befehls **Datei** > **Archivieren**) erstellt und enthält Steuerungsdateien des Programms, die zum Zeitpunkt der Archiverstellung aktuell waren, sowie die Postdatenbank.

Führen Sie folgende Schritte aus, um die Postdatenbank manuell wiederherzustellen:

1 Beenden Sie das Programm „Business Mail".

2 Falls ein Fenster mit der Meldung über fehlende Dateien im Ordner `\MS` und dem Vorschlag, einen neuen, leeren Ordner anzulegen, angezeigt wird, klicken Sie auf **Abbrechen** (s. Abbildung auf S. 172).

3 Wechseln Sie zu einem der Ordner mit der Erweiterung `REP` oder in den Ordner `\MSArch` (in Abhängigkeit davon, welcher dieser Ordner ein späteres Erstellungsdatum hat) und führen Sie eine der folgenden Aktionen aus:

  o Falls ein Ordner mit der Erweiterung `REP` gewählt wurde:

    - Kopieren Sie den gesamten Inhalt (Dateien und Ordner) des Ordners `\MS` an eine beliebige Stelle auf der Festplatte.
    - Kopieren Sie den gesamten Inhalt des Ordners mit der Erweiterung `REP` in den Ordner `\MS`.
  - Falls der Ordner `\MSArch` gewählt wurde:
    - Kopieren Sie den gesamten Inhalt des Ordners `\MS` an eine beliebige Stelle auf dem Laufwerk.
    - Kopieren Sie den gesamten Inhalt des Ordners `\MSArch` in den Ordner `\MS`.

4. Starten Sie „Business Mail".
5. Falls wieder eine Meldung über Fehler beim Öffnen der Postdatenbank eingeblendet wird, wiederholen Sie die Schritte **1-4**. Benutzen Sie dabei einen anderen Ordner mit der Erweiterung `REP` oder einen anderen Ordner `\MSArch`.
6. Wenn die weiter oben beschriebenen Schritte zu keinem Ergebnis geführt haben, dann können die beschädigten Daten nicht wiederhergestellt werden. Installieren Sie „Business Mail" neu und beginnen Sie, mit einer neuen Postdatenbank zu arbeiten.



Externe Datenträger

Allgemeine Informationen

Externe Geräte werden zum Speichern der Schlüsselcontainer verwendet. Diese Schlüsselcontainer können für die Authentifizierung, zum Erstellen von digitalen Signaturen (s. Digitale Signatur auf S. 178) oder für andere Zwecke verwendet werden.

Auf dem externen Gerät können Schlüssel gespeichert werden, die mit Hilfe unterschiedlicher Algorithmen in ViPNet Software oder in Drittanwendungen erstellt wurden. Die maximale Anzahl der Schlüsselcontainer, die auf einem externen Gerät gespeichert werden können, hängt von der Speicherkapazität des Geräts ab.

Die Software ViPNet Business Mail unterstützt zwei Arten der Authentifizierung mit Hilfe eines externen Geräts (s. Authentisierungsmodi auf S. 26):

- Mit dem privaten Schlüssel des ViPNet Benutzers, der auf dem Gerät gespeichert wird. Diese Art der Authentifizierung hat die folgenden Einschränkungen:
  - Ein externes Gerät kann nicht für die Authentifizierung mehrerer ViPNet Benutzer verwendet werden.
  - Ein externes Gerät kann nicht für die Authentifizierung eines Benutzers auf mehreren ViPNet Knoten verwendet werden.
  - Wenn diese Art der Authentifizierung verwendet wird, dann müssen die Signaturschlüssel des Benutzers, die mit Hilfe von ViPNet Software in der Zertifizierungsstelle erstellt wurden, auf dem gleichen Gerät wie der private Schlüssel gespeichert sein.
- Mittels Zertifikat, das gemeinsam mit dem entsprechenden privaten Schlüssel auf dem Gerät gespeichert wird.

Das Zertifikat für die Authentifizierung kann in der Windows-Domäne angefordert werden. Der Schlüsselcontainer wird dabei auf einem externen Gerät gespeichert, das den Standard PKCS#11 unterstützt.

Alle Operationen mit Schlüsselcontainern und externen Geräten können Sie im Programm ViPNet CSP durchführen. Damit ein externes Gerät auf dem Computer verwendet werden kann, sollten zunächst die Treiber dieses Geräts installiert werden. Stellen Sie vor dem Speichern der Schlüssel auf dem Gerät sicher, dass das Gerät formatiert ist.

Liste externer Datenträger

In der nachfolgenden Tabelle sind externe Geräte aufgelistet, die im Programm ViPNet Business Mail verwendet werden können. Für jedes externe Geräte werden die Beschreibung, die Bedingungen und Besonderheit der Verwendung sowie Informationen zur Unterstützung des Standards PKCS#11 aufgeführt.

Tabelle 5. Liste externer Datenträger

Name des Geräts in Software ViPNet CSP	Vollständiger Name und Gerätetyp	Anwendungsbedingungen	Unterstützung von PKCS#11
eToken Aladdin	Persönlicher elektronischer Schlüssel **eToken PRO (Java)**, **eToken PRO** vom Hersteller Aladdin.	Auf dem Netzwerkknoten muss die Software PKI Client 5.1 oder höher installiert sein. eToken PRO SmartCard kann mit jedem PC/SC-kompatiblen Smart Card Reader benutzt werden.	Ja
iButton Aladdin	Elektronischer Schlüssel **Dallas**, **iButton** Typ **DS1993**, **DS1994**, **DS1995** und **DS1996**.	Das Lesegerät muss an den Computer angeschlossen werden. Auf dem Computer muss die Software zur Datenübertragung mit iButton, 1-Wire Drivers Version 3.20 oder Version 4.0.3 installiert sein. In den Betriebssystemen Windows XP und Server 2003 kann neben ViPNet Software ausschließlich die Software 1-Wire Drivers Version 3.20 verwendet werden.	Nein
Smartcard Athena	Karten mit dem Speichertyp I2C (ASE M4), synchrone Karten mit dem Bustyp 2/3 und geschütztem Speicher nach ISO7816-3 (ASE MP42).	Das Auslesen und Eintragen der Daten auf Smartcard erfolgt durch den CardReader ASEDrive III PRO-S des Herstellers Athena. Die Treiber der Version 2.6 sollen auf dem PC installiert werden.	Nein

Name des Geräts in Software ViPNet CSP	Vollständiger Name und Gerätetyp	Anwendungsbedingungen	Unterstützung von PKCS#11
Siemens CardOS	SmartCards **CardOS/M4.01a,** **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** vom Hersteller Atos (Siemens).	Auf dem Computer muss die Software Siemens CardOS API V5.0 oder höher installiert werden.	Ja



Glossar

B

Benutzerrechte

Die Rechte, die dem Benutzer für Einstellungen in der ViPNet Software auf seinem Netzwerkknoten zugewiesen sind. Die Anmeldung mit dem Administrator-Passwort hebt jegliche Einschränkungen der Benutzer-Anmeldung auf.

Benutzerschlüssel

Eine Reihe von Dateien, die für die Authentifizierung des Benutzers notwendig sind. Der persönliche Schlüsselsatz wird in Abhängigkeit von der Authentisierungsmethode des Benutzers erstellt.

C

Client

Netzwerkknoten, der entweder einen Ausgangs- oder Endpunkt für die Datenübertragung darstellt. Im Vergleich mit dem Coordinator verfügt der Client über keine Routing-Funktionen.

D

Datei (Transportdatei)

Dienstinformation, die innerhalb des ViPNet Netzwerkes verwendet wird und durch das MFTP-Modul übermittelt wird.

Diffie-Hellman-Protokoll

Eines der Protokolle mit öffentlicher Schlüsselverteilung, bei welchem zwei Benutzer durch die dynamische Interaktion untereinander einen gemeinsamen geheimen Schlüssel erzeugen können. Es basiert auf dem Austausch offener (nicht verschlüsselter) Nachrichten ohne irgendwelche gemeinsame geheime Information, die im Voraus verteilt wird.

Digitale Signatur

Eine digitale Signatur ist ein kryptografisches Verfahren, bei dem zu einer „Nachricht (d. h. zu beliebigen Daten) eine Zahl (die digitale Signatur) berechnet wird, deren Urheberschaft und Zugehörigkeit zur Nachricht durch jeden geprüft werden können. Digitale Signaturen basieren auf asymmetrischen Kryptosystemen und verwenden folglich ein Schlüsselpaar, das aus einem privaten (geheimen) und einem öffentlichen (nicht geheimen) Schlüssel besteht.

N

Netzwerkknoten Administrator

Person, die für die Konfiguration des Netzwerkknotens verantwortlich ist.

Nutzdaten

Eine Datei, die durch die Anwendung „Business Mail“ bzw. „File Exchange“ erstellt wird, um diese an andere Netzwerkknoten weiterzuleiten.

O

Öffentlicher Schlüssel

Eine Reihenfolge von Zeichen, die zum privaten Schlüssel in bestimmter mathematischer Relation steht. Der öffentliche Schlüssel ist für alle Benutzer des Systems zugänglich und dient der Bestätigung der Echtheit einer digitalen Signatur (oder Verschlüsselung).

Ordner der Schlüsseldistribution

Ordner mit der Schlüsseldistribution.

P

Privater Schlüssel

Durch diesen Schlüssel werden andere Schlüssel, auf die der Benutzer Zugriff hat, geschützt. Er schützt die Information, die der persönliche Schlüssel beinhaltet. Er muss besonders gut aufbewahrt werden. Eine Kompromittierung dieses Schlüssels bedeutet automatisch die Kompromittierung aller Benutzerschlüssel.

R

Rolle

Eine Netzwerkknoten-Funktion, die eine Aufgabe im Rahmen eines ViPNet Netzwerks übernimmt. Rollen werden bei der Lizenzierung eines Netzwerks verwendet. Entsprechende Einträge in der Datei `infotecs.reg` bestimmen, über welche Funktionen der jeweilige Netzwerkknoten verfügt und welche Softwarekomponenten auf dem Knoten installiert werden dürfen.

Rollen können Attribute in Form von quantitativen Eigenschaften und Rechten haben, die ebenso die Funktionalität eines Netzwerkknotens bestimmen.

S

Schlüsseldistribution

Die Datei mit der Erweiterung `.dst`, wird im ViPNet Network Manager (in ViPNet VPN-Netzwerke) oder ViPNet Network Control Center (in ViPNet Netzwerke basierte auf der Software ViPNet Administrator) erstellt. Die Datei beinhaltet Schlüsselinformationen, Adresslisten und die Lizenzdatei, die für den initialen Start des Netzwerkknotens erforderlich sind.

Schlüsselordner

Der Ordner mit dem Benutzerschlüssel.

Sitzungsschlüssel

Zufälliger symmetrischer Schlüssel, der für die Verschlüsselung einer Nachricht bestimmt ist. Der erzeugte Sitzungsschlüssel wird seinerseits verschlüsselt und im Nachrichtenumschlag untergebracht. Das Format des Sitzungsschlüssels, der Algorithmus und der Vorgang seiner Verschlüsselung werden in RFC 4357 und RFC 4490 beschrieben.

T

Transportmodul (MFTP)

Die Software-Komponente für den Informationsaustausch innerhalb des ViPNet Netzwerkes.

V

ViPNet Key and Certification Authority

Eine der Software-Komponenten von ViPNet Administrator.

ViPNet Netzwerk

Mit Hilfe von ViPNet Software aufgebautes logisches Netzwerk.

ViPNet Netzwerkknoten

Computer mit installierter ViPNet Software.

Z

Zertifikat

Ein Digitales Zertifikat (auch Zertifikat oder Public-Key-Zertifikat) sind strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen. Durch ein digitales Zertifikat können Nutzer eines asymmetrischen Kryptosystems den öffentlichen Schlüssel einer Identität (z. B. einer Person, einer Organisation oder einem IT-System) zuordnen und seinen Geltungsbereich bestimmen. Damit ermöglichen digitale Zertifikate den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch die korrekte Anwendung der öffentlichen Schlüssel.

Zertifikatsanfrage

Eine Datei, in der der Benutzername im Format X.500, die Parameter des öffentlichen Schlüssels, erwünschte Gültigkeitsdauer des Zertifikats, Geltungsbereiche des Zertifikats, usw., enthalten sind (Zusammensetzung der Parameter hängt vom Format der Anfrage sowie von der Software ab, in welcher die Anfrage erstellt wird).

Die Anfrage kann sowohl zur Ausstellung eines neuen als auch zur Aktualisierung eines bestehenden Zertifikats erzeugt werden.

Zertifizierungskette

Eine geordnete Abfolge von Zertifikaten, die der Hierarchie der Herausgeber dieser Zertifikate entspricht. Das Zertifikat wird als gültig eingestuft, wenn die Zertifikatskette vollständig ist (d. h. durch ein Stammzertifikat abgeschlossen ist) und alle darin erfassten Zertifikate ebenfalls gültig sind.



Index

A

B

C

D

E

N

O

R

S

T

V

Z